C 73/3

U.S. Department of Justice
Bureau of Justice Statistics

NEWARK PUBLIC LIBRARY
OCT 9 1981
U. S. GOVT. PUBS.

COMPUTER CRIME

Expert Witness Manual

READEX FICHE

best copy available

J 29.8:

U.S. Department of Justice
Bureau of Justice Statistics

Benjamine H. Renshaw
Acting Director

Carol G. Kaplan
Director,
Privacy & Security Staff

U.S. Department of Justice
Bureau of Justice Statistics

Computer Crime

Expert Witness Manual

This document was prepared for the Bureau of Justice Statistics (BJS), U.S. Department of Justice (DOJ) by Koba Associates, Inc. under Contract No. J-LEAA-007-80. Points of view and opinions stated herein are those of the authors and do not necessarily represent the official position or policies of BJS, DOJ or Koba Associates, Inc.

© Copyright 1980 by Koba Associates, Inc.

BJS authorizes any person to reproduce, translate or otherwise use any or all of the copyrighted materials in this publication with the exception of those items indicating that they are copyrighted by or reprinted by permission of any source other than Koba Associates, Inc.

FOREWORD

As the criminal justice system is confronted with increasing levels of computer related crime, and as efforts increase to bring sophisticated felons to justice, the use of expert witnesses will represent an invaluable source of technical assistance to investigators and prosecutors. This Manual attempts to examine many of the issues, factors and obstacles which may surface in the use of expert witnessses. Criminal justice personnel contemplating the use of an expert witness would be well advised to sensitize themselves to the issues raised within this document.

As technology advances complicate the matters of evidence and testimony in computer related crime cases, the use of experts will become more and more prevalent. However, it is important to remember that technical expertise can only be made effective when skillfully directed by well-informed and capable criminal justice practitioners. It is for you, the practitioner, that the Expert Witness Manual is intended.

Benjamin H. Renshaw
Acting Director
Bureau of Justice Statistics

PREFACE

The Expert Witness Manual is a simple, easy to understand reference tool that guides those individuals who need the assistance of experts in computer related crime investigations and prosecutions. It outlines for the reader how he/she should proceed in the expert's selection. The Manual also details the economics that should be considered in the selection of an expert. It suggests sources which can be employed to tap an expert, and how best to use these resources.

Further, the Manual details how best to employ and manage an expert. It proceeds to define the legal powers of the expert, and the potential legal liabilities that can ensue from the expert's activities. This Manual should prove of special value not only to investigators, but also prosecutors and defense attorneys; it outlines the economics of using computer experts at both the pretrial and trial stages.

The Expert Witness Manual was written for both the public and private sectors. It should prove of value not only to police officials and prosecutors, but also to defense attorneys, private consultants, corporate managers, accountants, internal auditors, private investigators, students of criminology, and many others. It marks a serious effort to assist both the private and public sectors in combatting computer crime.

August Bequai, Esq.
Washington, D.C.
Fall, 1980

TABLE OF CONTENTS

Section Page

Foreword.. i

Preface... ii

1.0 Introduction and Executive Summary.................... 1

- 1.1 Purpose and Scope of This Manual.................. 1
  - 1.1.1 Use of The Manual.......................... 1
  - 1.1.2 Organization of the Manual................ 2
- 1.2 Overview of the Problem........................... 3
  - 1.2.1 Definition of Computer Related Crime....... 3
  - 1.2.2 Nature of the Phenomenon in the Context of White Collar Crime............ 5
  - 1.2.3 Unique Aspects of Computer Related Crime.................................. 8
  - 1.2.4 Scope of the Problem Nationally............ 10
  - 1.2.5 Vulnerability of Computer Systems With the Growth of Computer Technician Cadres....................... 11
- 1.3 Investigative and Prosecutive Approaches to Computer Related Crime...................... 12
  - 1.3.1 Case Complexity and the Need for Technical Assistance.................... 12
  - 1.3.2 Problems Arising From the High Technology Aspects of Computer Related Crimes.......................... 13
  - 1.3.3 The Multi-disciplinary Team Approach to Computer Related Crime Investigations.... 14
  - 1.3.4 Utility of Outside Experts Assisting With Aspects of the Computer Related Crime Case............................. 15
  - 1.3.5 Caveats and Recognized Limitations on the Use of Outside Experts.............. 16

2.0 Defining the Expert and His or Her Role............... 19

- 2.1 "Expert" Defined.................................. 19
  - 2.1.1 Expert Witness Defined..................... 20
  - 2.1.2 Roles of Expert Consultant and Expert Witness Distinguished for the Purpose of This Manual.......................... 20

Table of Contents (Continued)

Section

Page

2.2 Types of Expertise Distinguished by Source of Expert........ 20
  2.2.1 The Confidential Informant/Technical Adviser........ 22
  2.2.2 The "Loaned" Government Employee........ 22
  2.2.3 The "Provided" Consultant........ 23
  2.2.4 The Retained Consultant........ 24
  2.2.5 The Court Appointed Expert........ 24
2.3 Types of Expertise Distinguished by Subject Area Specialities........ 25
  2.3.1 General Experts........ 27
    2.3.1.1 Computer Scientists........ 27
    2.3.1.2 Computer Related Crime Researchers and Scholars........ 27
  2.3.2 Subject Matter Experts from Various Data Provider and Computer User Communities........ 27
  2.3.3 Computer Technologists........ 29
    2.3.3.1 Electronics Engineers........ 29
    2.3.3.2 Telecommunications Engineers........ 29
    2.3.3.3 EDP Programmers........ 30
    2.3.3.4 Systems Analysts........ 30
    2.3.3.5 Database Managers........ 30
  2.3.4 EDP Auditors........ 31
  2.3.5 Computer Security Specialists........ 31
  2.3.6 Hardware and Software Manufacturers and/or Vendors........ 32
  2.3.7 Computer Service Representatives........ 32
  2.3.8 Experienced Computer Related Crime Investigators and Prosecutors........ 33
  2.3.9 Forensic Scientists........ 33
    2.3.9.1 Forensic Chemists........ 33
    2.3.9.2 Document Examiners........ 33
2.4 Summary Overview of the Role of the Expert in a Computer Related Crime Case........ 34

Table of Contents (Continued)

Section Page

3.0 When to Employ an Expert.............................. 35

- 3.1 Computer Related Crime Cases Vary Greatly in Complexity and Type.......................... 35
  - 3.1.1 Need for Technical Assistance Will Depend on Case Type, Complexity.......... 35
  - 3.1.2 Number and Type of Experts Needed Will Depend on Case Type and Complexity....... 38
- 3.2 Philosophy and Capabilities of the Law Enforcement Agency Will Impact on the Use of Expert Assistance........................... 39
  - 3.2.1 The Reactive Approach to Law Enforcement... 40
  - 3.2.2 The Proactive Approach..................... 41
- 3.3 Look First to In-House Resources.................. 42
- 3.4 Factors That Will Determine Whether and Where to Turn to Outside Expert Assistance............ 43
  - 3.4.1 Nature and Complexity of the Case.......... 43
  - 3.4.2 Case Sensitivity........................... 43
  - 3.4.3 Previous Experience With the Use of Experts.................................. 45
  - 3.4.4 Fiscal and Budgetary Considerations........ 46
  - 3.4.5 Availability of Local Resources............ 46

4.0 Selecting an Expert................................... 47

- 4.1 Financial Considerations.......................... 47
  - 4.1.1 Availability of Funds...................... 48
  - 4.1.2 Reasonable Compensation Levels............. 49
  - 4.1.3 Balancing the Competing Interests.......... 52
- 4.2 Requisite Qualifications Will Vary With The Expert's Speciality Area.................... 54
- 4.3 General Criteria and Standards for Evaluating An Expert's Qualifications........... 56
  - 4.3.1 Credentials................................ 56
    - 4.3.1.1 Professional Licensure, Certification or Registration........ 57
    - 4.3.1.2 Academic Degrees.................. 58

Table of Contents (Continued)

Section

Page

- 4.3.1.3 Training and Continuing Education Experience............ 61
- 4.3.1.4 Writings and Publications......... 61
- 4.3.1.5 Teaching and Other Consultancies.................. 62
- 4.3.1.6 Professional Associations......... 63
- 4.3.1.7 Previous Similar Experience....... 63
- 4.3.1.8 Access to Privileged Information or Unique Facts................ 64

4.3.2 Personal Qualities of the Expert........... 65

- 4.3.2.1 Ability to Work as Part of a Team......................... 65
- 4.3.2.2 Trustworthiness and Integrity..... 65
- 4.3.2.3 Professional Reputation and Recognition..................... 66
- 4.3.2.4 Quality and Timeliness of Previous Work.................. 66
- 4.3.2.5 Professional Bearing and Demeanor....................... 67
- 4.3.2.6 "Presence" Before a Group......... 67
- 4.3.2.7 Articulation with Laymen.......... 68
- 4.3.2.8 Mannerisms and Idiosyncracies..... 69

4.4 Sources for Indentification of Individual Experts.................................... 69

4.5 Distinguishing the True Area of Competence........ 70

5.0 Privacy and Security Considerations in the Use of Outside Experts.................................... 73

5.1 Privacy and Security Considerations in Computer Related Crime Investigations........... 73

5.2 The Necessity for Background Checks and Credibility Evaluations....................... 74

5.3 Key Steps in Completing the Background Check...... 75

5.4 Special Security Precautions During the Course of the Investigation.......................... 76

- 5.4.1 Limiting Access to Sensitive Information to "Need-to-Know" Personnel............. 76
- 5.4.2 Utilizing Multiple Experts as a Cross-Check on Each Other..................... 77

Table of Contents (Continued)

Section Page

5.4.3 Reliance on Technological Aids............. 77
5.4.4 Deputizing the Expert...................... 78

5.5 Weighing Credibility Factors...................... 79
5.6 Establishing Security Within the Investigative Unit.............................. 80
5.7 Positive Approaches Toward Preventing Breaches of Security........................... 81
5.8 Legal Remedies for Breaches of Privacy or Security by an Expert........................... 82

5.8.1 Illegal Acts Against a Computer or Its Software............................ 84
5.8.2 Misuse of Confidential Information......... 84
5.8.3 Unlawful Out-of-Court Disclosures.......... 85

5.8.3.1 Federal Statutes.................. 85
5.8.3.2 State Statutes.................... 87
5.8.3.3 Tortious Liability................ 87
5.8.3.4 Breach of Contract................ 89

5.8.4 Breaches of Special Privileges............. 89
5.8.5 Violations of Specific Computer Security Laws........................... 91

6.0 Utilizing the Expert in All Phases of the Case......... 93

6.1 Preliminary Investigative Work.................... 93
6.2 The Pretrial Stage................................ 94
6.3 Litigation Support and Expert Testimony........... 96

7.0 Managing the Expert...................................101

7.1 General Management Considerations for All Phases of the Case.............................101

7.1.1 Establishing Rapport and An Atmosphere of Trust at the Outset..................101
7.1.2 Integrating the Expert Into the Major Case Investigative Team..................102
7.1.3 Determining, In Conjunction with the Expert, All Facets of His "Negotiated Collaboration" with the Investigation....103
7.1.4 Determining in Advance the Scope of the Expert's Tasks to be Performed..........103

Table of Contents (Continued)

Section

Page

7.1.5 Fixing Responsiblity for Guidance and and Direction of the Expert..............104
7.1.6 Agreeing to Level of Compensation, Fee Arrangement, Work Schedule, Deliverables and Payment Plan............104
7.1.7 Formalizing the Terms and Conditions of the Expert's Utilization in A Written Agreement........................106
7.1.8 Quality Controls..........................107
7.1.9 Security Considerations...................107

7.2 Special Management Considerations at the Trial Stage..................................108

7.2.1 Review of the Expert's Views, Writings, Prior Statements for Consistency.........108
7.2.2 Review of the Expert's Credentials and Views in Preparation for Laying the Foundation...............................109
7.2.3 Rehearsal of Expert Testimony to be Given on Direct Examination..............109
7.2.4 Preparing the Expert Witness for Cross Examination............................110
7.2.5 Anticipating Defense Objections and Impeachment Tactics.....................110

Footnotes..115

Bibliography...121

Appendix A--Significant Issues in Federal Expert Witness Law..................................A-1

Appendix B--Federal Pretrial and Trial Discovery Issues Applicable to Computer Related Crime Cases......B-1

Appendix C--Federal and State Cases Regarding Use of Expert Witnesses..............................C-1

Appendix D--Selected State Privacy Laws Applicable to Computer Security.............................D-1

1.0 INTRODUCTION AND EXECUTIVE SUMMARY

Complex computer related crimes may present substantial difficulties for criminal justice practitioners involved in their investigation and prosecution. In some cases, the use of expert witnesses may be essential to successfully bringing sophisticated felons to justice. The Expert Witness Manual is designed to serve as the "first step" in familiarizing criminal justice personnel with the issues associated with the use of expert witnesses.

1.1 Purpose and Scope of This Manual

The Manual is intended as an aid when assessing the need for technical assistance in a computer related crime case. Should a need for outside expertise be determined to be present in the case, the Manual is intended further to serve as a guide for how to identify, select, manage, and utilize such experts and how to avoid common pitfalls encountered when using outside resources.

The importance of utilizing technical assistance at key stages in the computer related crime case has been stressed previously by the U.S. Department of Justice. The recently published Computer Crime Criminal Justice Resource Manual aptly notes that

> [c]omputer related crimes deal with people to a far greater degree than they deal with technology. Only people, and not computers, perpetrate, witness or are the ultimate victims of these crimes. Therefore, investigators and prosecutors need to know more about the people and their functions in electronic data processing (EDP) than about the computer technology. Technical assistance can be obtained from experts.[1]

1.1.1 Use of the Manual

Investigators and prosecutors should value this Manual for its "how to" approach to the use of technical experts in a major computer related crime case. In this regard, the Manual goes beyond a strictly legalistic treatment of the subject by also considering ethical issues, management and supervision problems, privacy and security concerns and other important areas relating to the use of experts in a major case investigation.

Without question, issues relating to the applicable substantive law, rules of evidence and criminal procedure must hold center stage during the case preparation and trial stages. But legal issues are not the only important issues.

Matters relating to the identification, management and effective utilization of technical experts can be equally important when "breaking" a computer crime case. This is especially true because the overwhelming number of such cases that have been reported have been disposed of out of court, sometimes informally, without direct intervention by the criminal justice system. Consequently, there are few cases where the use of expert witnesses at trial and the admissibility of expert testimony have been central to the effective use of outside experts to "break" such cases.

Further, because the Government must build its computer crime cases, like other cases, on the supposition that it will have to go to trial and sustain its burden of proof, the potential expert witness who may be called at trial in most instances will have already been involved behind the scenes, working as a consultant or technical adviser at the investigative and/or pretrial stages. Thus, the non-legal aspects of this Manual will also have applicability for use of expert witnesses at the trial stage. It should be noted that the Manual is not intended as and should not be viewed as an inclusive discussion of the rules and conventions governing the use of experts in all jurisdictions. Law enforcement personnel are advised to employ the Manual for general background purposes, and to consult State and local codes and regulations in connection with any attempt to retain the services of expert witnesses. It should also be pointed out that the Manual has applicability for private investigators as well as for their public sector counterparts. In this regard, many of the issues raised as concerns of the Government should be considered germane to private sector investigatory efforts.

1.1.2 Organization of the Manual

The organization of this Manual is designed to facilitate easy reference by investigators and prosecutors faced with real or apparent computer related crimes. Sections address topics in the order they would be mostly likely to arise. Section 2.0 defines what is meant by an expert, distinguishes the various sources of experts for computer related crime cases, and discusses subject area specializations among experts which are recommended to be tapped for such cases.

Section 3.0 addresses the question of when to employ an expert. Considerations of case complexity and the individual law enforcement agency's philosophy and capabilities are presented. The Section concludes with a review of key phases in a computer related crime investigation at which expert assistance will most likely be required.

Section 4.0 presents the major considerations that should be kept in mind when selecting a particular expert or team of experts. Financial considerations are addressed, and requisite professional and personal qualifications are detailed. General sources which can aid in identifying outside experts are presented.

Section 5.0 details privacy and security considerations which are of importance when selecting and utilizing outside experts. Background checks and other special security precautions are discussed. The advantages and disadvantages of deputizing the technical adviser are also presented. Overall measures to be taken to avoid breaches of security are suggested, and remedies for breaches of privacy and security by outside experts are also discussed.

Section 6.0 discusses utilizing the expert in all phases of the case. The key points at which outside assistance is likely to be needed, which were initially presented in Section 3.0, are addressed more purposefully here. Critical points for using experts are grouped by whether they occur at the investigative, pretrial, or trial stages.

Section 7.0 presents recommended techniques for managing experts throughout the course of a major case, with special attention given to the litigation stage.

1.2 Overview of the Problem

Computer related crime has been variously defined. This Section analyzes several contrasting definitions. Unique features of computer related crime which tend to distinguish it from other offenses are presented, while the basic interrelationship between computer related crime and "white collar" crime is stressed. The scope of the problem nationally is estimated, and the potential for increasing levels of computer abuse and computer fraud due to the rapid growth of a skilled computer technologist class and the lack of computer security is underscored.

1.2.1 Definition of Computer Related Crime

At present there is no universally accepted definition of computer related crime. However, authorities and commentators agree that the nature of this new form of technological crime goes beyond mere computer abuse; most computer related crimes directly involve the use of a computer to commit acts which the law has already defined as criminal.

Computer related crime has been variously characterized as using a computer to steal money, services, or property, or to commit an invasion of privacy, or an act of extortion or terrorism. Recently proposed Federal legislation on the subject includes within the scope of its prohibitions (a) directly or indirectly accessing, or attempting to access, any computer system to (1) devise or execute a scheme to defraud, or (2) obtain money, property or services by means of false or fraudulent pretenses; and (b) actual or attempted intentional and unauthorized alteration, damage, or destruction of any computer or its software, program or database.2/

Given the ongoing advances in computer technology and the ever increasing applications of computers in our daily lives, even these attempts at definitions are not all-encompassing. Leading authorities recently have promulgated broader definitions. These include the following:

- "[A]ny illegal act for which knowledge of computer technology is essential for successful prosecution", which thus includes "crimes and alleged crimes (which) may involve computers not only actively but also passively, when usable evidence of the acts resides in computer stored form"3/; and
- "the use of a computer to perpetrate acts of deceit, concealment and guile that have as their objective the obtaining of property, money, services, and political and business advantages", as well as "threats or force directed against the computer itself . . . usually sabotage or ransom cases", all of which acts "have one commonality--the computer is either the tool or the target of the felon."4/

Though these two definitions largely overlap, they are not entirely congruent. This points out the problem that arises when trying to either inclusively or exclusively define computer related crime. For example, the theft of computer hardware under the first definition would not, in and of itself, constitute a computer related crime. As one leading authority has argued,

> [i]f a computer is stolen in a simple theft where based on all circumstances it could have been a washing machine or a milking machine and made no difference, then a knowledge of computer technology is not necessary, and it would not be a computer related crime.5/

Under the second definition, however, the theft of computer hardware probably would constitute a computer related crime. Certainly the theft of a valuable computer program would fall within this broader of the two definitions. The noted proponent of this more encompassing definition also includes attempts to destroy a computer with explosives or firearms as computer related crimes.6/

The problem of definition is advanced here for one primary reason: Not all cases which involve a computer are necessarily technologically complex. While, as we have seen, some authorities would include thefts of computer hardware or software as well as acts of sabotage or vandalism committed against a computer within the definition of computer related crime, law enforcement personnel probably would not need to know a great deal about computer technology, if anything, to successfully investigate and prosecute such crimes. Computer related crimes, then, can and do run the entire spectrum of case complexity. This fact will be of central importance when deciding on investigative and prosecutive approaches to computer related crime cases and the need for bringing specialized experts into the case, as discussed in Section 1.2.3, below.

1.2.2 Nature of the Phenomenon in the Context of White Collar Crime

Computer related crime is not a traditional crime, even though its perpetrators may be charged under pre-existing larceny, embezzlement or fraud statutes. Most computer related crime falls within various areas of "white collar crime," as distinct from acquisitive "street crime." The overlap between computer related crime and white collar crime is substantial, and an understanding of the illicit motivations of the white collar criminal is important when attempting to understand the nature and scope of computer related crime.

The term "white collar crime" was first coined by Edwin H. Sutherland in his 1949 publication, White Collar Crime. Sutherland developed a definition of the term that related primarily to offenses committed by "respectable" persons, usually in the course of and related to their occupations.[7] In the ensuing years, we have come to understand the term in a much broader context. White collar crime is now defined as an illegal act or series of illegal acts normally committed by non-physical means and by concealment or guile, to obtain money or property, to avoid payment or loss of money or property, or to obtain business or personal advantage. It may be carried out singly or by two or more individuals conspiring to plan, initiate and carry out the offense. White collar offenses may also include violation of regulations developed by Federal, State, or local agencies under their appropriate statutory authorities. Examples of this type of offense include the violation of regulations issued in the area of securities, welfare, commerce, environment, and energy.[8]

Some other critical areas of white collar crime include infiltration of legitimate business by organized crime elements for illegal purposes and commercial bribery and other competitive procurement frauds to obtain unfair advantage (including kickbacks, bid-rigging and other forms of collusion which may occur in either the public or private sector, especially the fraudulent transfer of securities and stocks). To the extent that computers are used to perpetrate these crimes--which is increasingly the case-- there is a major overlap between computer related crime and white collar crime.

According to a recent Report released by the Bureau of Justice Statistics, computers can play any of four roles in the commission of a crime.[9] These are illustrated in Table 1, following.

Table 1

Roles Computers Can Play in Commission of A Crime

Computer As Object:	The purpose of the crime can be to destroy, damage or hold for ransom the computer facility itself, computer hardware, computer programs, the computerized data base, or printouts of valuable data.
Computer As Subject:	A computer can be the site or environment of a crime. Illicitly gained assets or stolen information can be stored indefinitely in the computer for later use.
Computer As Instrument:	Complex financial schemes to defraud can be accomplished by using the computer as a tool or instrumentality of the crime, either actively (e.g. by transferring assets) or passively (e.g. by creating a false record of corporate assets to mislead outsiders as to the financial stability of a corporation).
Computer As Symbol:	The computer can be used to create a record which when presented to the victim serves to intimidate or deceive him into parting with something of value.

With the exception of malicious destruction and political terrorism, the vast majority of reported computer related crime cases amount to one or another form of acquisitive white collar crime. Table 2 illustrates the major categories of white collar computer crimes.

Table 2

Major Categories of Computer Related Crimes
As Functions of White Collar Crime

INDUSTRIAL SABOTAGE, ESPIONAGE & EXTORTION BY COMPUTER:

- Example: destruction or theft of competitor's confidential computer programs
- Example: sale of printouts to competitors by employees
- Example: scanning data base for confidential business information

DEFRAUDING PUBLIC THROUGH SYMBOLIC IMAGERY CREATED BY COMPUTER:

- Example: dissemination of bogus bills and collection notices
- Example: false advertising of non-existent computerized services

FINANCIAL CRIMES AGAINST BUSINESS BY COMPUTER:

- Example: complex financial swindles
- Example: creation of record of ficticious assets to enhance corporate standards
- Example: embezzlement of business assets by transference to another account
- Example: payroll thefts through alteration of time and salary records

DIVERSION AND THEFT OF NON-LIQUID ASSETS BY COMPUTER:

- Example: re-routing of rolling stock, freight, or cargo to alternate destination
- Example: tampering with fuel allocations

UNAUTHORIZED USE OF THE COMPUTER BY EMPLOYEES FOR ILLICIT PURPOSES:

- Example: illegal betting schemes

The technological methods used to commit computer related crimes of the white collar type are new. However, considerable research has been undertaken which has grouped and classified these techniques. Like other aspects of this high technology subject, a specialized vocabulary has ~~grown up~~ to describe such practices. For a description and explanation of 12 classical methods to perpetrate a computer related crime of the high technology, white collar crime sort, together with an outline of potential perpetrators, methods of detection, and evidence associated with each, the reader is referred to BJS' recently published Computer Crime Criminal Justice Resource Manual.10/

1.2.3 Unique Aspects of Computer Related Crime

Notwithstanding its similarity in many respects to other forms of white collar crime, there are many unique aspects to computer related crime which make its investigation and prosecution difficult. These include the following:

- Losses from acquisitive computer related crimes are enormous when compared to the time and physical effort invested in their perpetration. One recent study of several hundred computer criminals found the average "take" to be $400,000.11/
- The victims of computer related crimes--generally business and industry--are reluctant to report such crimes, despite major losses, for fear of adverse publicity, loss of stockholder confidence, etc. Victim cooperation with the investigation can, as a result, be minimal.
- Computer crimes are generally of low visibility and, consequently, are difficult to detect. As a former U.S. Attorney General noted with regard to such offenses, "[t]here are no smoking pistols, no blood-stained victims; often the crime is detected by sheer accident."12/
- Computer related crimes can be committed over vast distances and across many intranational and international jurisdictional lines. Through the use of a remote computer terminal and telephone hook-up, a knowledgeable computer felon can, provided he knows how to access the system, give illicit instructions to a computer literally anywhere in the world.
- A large proportion of computer related crimes are "inside jobs." The opportunity for enormous financial gain, when set against the low risk of discovery

and leniency of punishment should one be caught, provides temptations for top management, computer technologists, and providers and users of computerized data alike to manipulate the computer for illicit gain.

- Computer criminals are most often well-educated, highly-skilled amateurs. They generally have no prior criminal history and are well-respected members of the community.

- Illicit gain is often not the only, or even primary motive, of computer criminals. The challenge of penetrating computer security safeguards in an effort to "beat the system" has also been suggested as a major motive of the lone computer felon. Taking adequate preventive action in this regard is extremely difficult.

- Once the crime has been detected, discovering and understanding the modus operandi in a technologically-complex computer related crime case can also be extremely difficult.

- As with other forms of white collar crime, law enforcement personnel will often identify a suspect in a computer related crime case before determining how the crime was committed and with what offense(s) to charge the suspect. How to charge a computer related crime can prove difficult when traditional crime statutes must be relied upon, within whose provisions technological crimes must be made to fit by implication.

- Establishing the timing of a computer related crime is often impossible. Computers can be instructed by electronic impulses to add, transfer or, as in case of detection, destroy key bits of information within a matter of a few milliseconds.

- Investigators frequently encounter difficulty in obtaining physical evidence in such cases. Drafting sufficiently specific subpoenas and translating computer-stored data which evidences a criminal act into human-readable form, without at the same time damaging the computer program or interrupting the ongoing business activities of the victim, can present major problems.

- Investigators experienced in other sorts of complex financial investigations are generally trained to follow a paper trail of audited financial reports in order to discover and pinpoint irregularities. Because of the very nature of computer operations--using electronic impulses to transfer information--there exists no "audit trail" in computer fraud cases.

- Computerized information which evidences a crime and which is stored in the computer's memory core on magnetic tapes can easily and quickly be altered or destroyed, often leaving no trace of tampering. Improper handling or storage can also damage such evidence. As a result, search and seizure problems, chain of custody problems, and evidence preservation problems in computer related crime cases can assume greater than normal significance.

- Admissibility of evidence problems abound. Because computer printouts and magnetic tapes are generally not original records but rather copies made from manual records after a time lag, prosecutors may encounter at least threshold difficulty in obtaining their admission into evidence at trial due to the Best Evidence Rule. Because two or more examples of such items to the human eye can be, and often are, indistinguishable from each other, authentication problems and chain of custody problems can also impede their admissibility into evidence. Because a computer printout generally will be introduced into evidence to support the truthfulness of its contents, it may be held to be inadmissible under the Hearsay Rule. Even if held potentially admissible under the Business Records Exception to the Hearsay Rule, the time lag experienced between the point at which the data was originally amassed and the point at which it was fed into the computer--often at another location--can run afoul of the "regular course of business" and "reasonable time" requirements of the Business Records Exception.

- The high technology aspects of a computer related crime are often difficult to explain in simplified terms and can prove difficult for the layman to understand. These communications problems can impact negatively on the trier of fact, whether judge or jury.

1.2.4 Scope of the Problem Nationally

The number of computers in use has doubled in the past 10 years, and with the advent of the mini-computer, use can be expected to quadruple within the next five years. At present, there are over two million men and women who operate more than 90,000 computers in this country. As August Bequai notes, they constitute a large and growing army in both business and Government. Such cadres of computer technologists now exist in all the developed nations, as well as in many developing ones.

Today, there is no large firm that does not use computers. There is no one individual whose life is not affected by computers.

It was estimated in 1972 that in the following 15 years the world-wide yearly gross losses through computer abuse would be 160 million dollars.[13] Present day estimates put the annual loss in this country alone at in excess of $100 million.[14]

Computer related crime is increasingly becoming a major public concern, from the standpoint of both prevalence and cost. The potential for further abuse is limitless due to the development of the technology for a "cashless society", also known as the Electronic Funds Transfer System (EFTS), which seeks to replace paper currency with "electronic impulses". (EFTS is the transfer of data relating to financial transactions over a series of communication networks. It begins with the input at the point of sale and culminates in computerized bookkeeping at a bank many miles away. EFTS represents the movement of funds from the account of the buyer to that of the seller, or from that of an employer to that of the employee.) The system will create a network of many computers and terminals that will be used to relay data of all types.[15]

The number and frequency of computer related crimes in our society is a subject of considerable controversy. This stems in part from the newness of the phenomenon--the first reported instance of computer abuse dating from as recently as 1958.[16] It also stems from the fact that many--perhaps most--computer related crimes go undetected or, once detected, unreported. A leading scholar gathered anecdotal information as well as data from case filings on almost 700 reported computer related crimes.[17] The recognized authority who estimates domestic reported computer related crime to amount to $100 million dollars annually regards this as "only the tip of the iceberg" and suggests that fewer than one percent of all computer crimes are uncovered.[18] All commentators agree, however, that the problem has reached serious proportions and is growing worse.

1.2.5 Vulnerability of Computer Systems With the Growth of Computer Technician Cadres

The tremendous growth of computer operations and the computer services industry have created the need for thousands of sensitive positions of trust within public and private sector agencies. Performance of the various technical and managerial functions required in the day-to-day operation of computerized systems places thousands of well-educated, highly-trained professionals in situations where computer manipulation for illicit gain can be perpetrated.

The over-abundance of trained computer technologists often leads to over-qualified employees filling low level computer related positions which require only routine skills. Frustration, boredom and resentment for many of these employees can lead to computer abuse. For others, the opportunity presented by lack of computer security and/or minimal supervision, when coupled with access to the computer to perform critical functions, creates too great a temptation to manipulate the computer for illicit gain. For still others, the challenge of outwitting a computer's sophisticated security systems is the primary motive.

A 1976 study which analyzed the crimes of 25 known computer related crime perpetrators underscores the fact that computer criminals almost invariably perform such illegal acts while on the job and that the type of computer related crime committed was generally that for which their skills, knowledge and accessibility most equipped them.19/ The study further suggested that the more autonomous the job function and the more vulnerable the computer system to unauthorized access or data altering, the greater the chance for computer related crimes to occur.

1.3 Investigative and Prosecutive Approaches to Computer Related Crime

In most respects, computer related crimes are not unique. While the "stakes" are usually higher or the "take" larger, as was noted earlier, many computer related crime cases parallel more traditional acts of damage to property, theft, extortion, terrorism, etc. in all key respects. The approach to investigating and prosecuting such cases, then, should also comply with sound traditional case management techniques. Some computer related crimes equal or exceed in complexity other forms of high technology crime and other types of white collar financial crime. The approach to investigating and prosecuting these more complex varieties must build upon accepted major case investigation techniques.

1.3.1 Case Complexity and the Need for Technical Assistance

The complexity of the computer related crime under investigation will have an important bearing on the decision whether, and if so, when to seek special expertise and assistance. In addition, the pre-existing sophistication, knowledge base and capabilities of local law enforcement personnel must be accessed, as well as the investigative agency's method of operation in the investigation and prosecution of these types of white-collar crime cases, before the decision is made to seek outside assistance.

The less complex and involved the case under the analysis, the further investigators without special training will be able to move forward without reliance upon specialized outside advice or assistance. This assumes, of course, that a minimal level of understanding of computers and of sound principles of investigation exists on the part of the investigator(s), even though the two skills have not necessarily been previously employed in combination on such an assignment. Without such a basic capability, obviously the situation analysts (investigators) would not be in a position to competently conduct even a superficial early assessment of the relative complexity of the case.

Perhaps the most straightforward example of such a basic need level would be a situation in which the computer has been the object of an attack (criminal damage to property) by an identified disgruntled employee. Basically, the requirements of such a case might not involve a great deal more than crime scene processing, preservation of evidence and conducting interviews to determine motive, amount of damage, and so forth. This situation would be in sharp contrast to the high technology skills and understanding needed to conduct the investigation of an ongoing computer related fraud perpetrated by unknown individuals, where merchandise inventories are being unlawfully diverted to fictitious businesses through the illegal entry and manipulation of a firm's computer system.

These contrasting examples point out different case investigative requirements. In the first example, a technical adviser, perhaps loaned from the equipment vendor or employee of the victim company, might be needed only toward the end of a relatively routine investigation. However, in the second example, highly specialized technical assistance would be required from a number of different disciplines, and from the very early planning stages of such a case right through to trial.

1.3.2 Problems Arising From the High Technology Aspects of Computer Related Crimes

As noted in Section 1.1.3, above, there are several unique aspects to complex computer related crimes. Problems arising from these high technology aspects of computer related crime generally cluster in the following areas:

- Detection Problems: The low visibility of most computer crimes which involve manipulation of data and/or transference of assets militates against detection except by accident. Even once discovered, determination of modus operandi can prove very difficult.

- Evidentiary Problems: Because computers transmit information by electronic impulses and store data in non-human-readable form, a host of evidentiary problems arise for investigators which run from search and seizure to data conversion, evidence preservation, chain of custody, authentication and admissibility at trial.

- Choice of Law Problems: Most jurisdictions do not as yet have computer crime statutes on the books. Selecting traditional criminal statute(s) under which to "fit" the offense so as to charge a suspect, and on which to base the prosecution, may prove difficult, depending on the facts and circumstances of the case.

- Comprehension Problems: Computer technology, like other subject areas, has its own jargon. Simplifying the nature of computer operations in a given case for legally-trained "laymen" (investigators and prosecutors) to follow during the early stages of the case is compounded when faced with the problem of simplifying the facts and circumstances for effective presentation to a jury.

In each of these major problem areas, a resort to outside technical assistance by investigators and prosecutors may prove useful and even necessary.

1.3.3 The Multi-disciplinary Team Approach to Computer Related Crime Investigations

In recent years law enforcement agencies have increased, with notable successes, the use of multi-disciplinary teams in major crime investigations. Experienced trial assistants from the prosecutor's office have teamed up with seasoned detectives and other investigators to form successful "career criminal" units and to plan and execute "operation sting" type operations, many of which have had primarily white collar crime orientations. The use of non-investigator specialists--whether confidential informants, forensic experts, or technical advisers--as part of such teams has also become commonplace.

Even more than is the case for other complex white collar crime investigations, computer related crimes can be expected to require the assistance of technical experts in addition to investigative and prosecutorial resources. The interdisciplinary team approach is advocated for the effective investigation and prosecution of such cases. Such a team concept envisions the very early involvement and continuing participation by an experienced criminal prosecutor. In addition, a staff of investigators and electronic data processing (EDP) auditors is essential, with other experts available for assistance in specialized areas, as required, over the course of a lengthy case.

Once an outside consultant or expert is brought onto the team, a special trust relationship must be established based upon informed judgements. That is to say, the expert, once so employed, must be recognized as a privileged insider and the criminal justice professionals must guard against generalizing from the expert's special knowledge to the areas of security consciousness or assuming integrity where there may not be a factual basis for that assumption absent reasonable inquiry.

Succeeding chapters of this Manual will address procedures for selecting experts for the investigative team, the roles such experts should play, privacy and security considerations in their use, and management techniques which should be adhered to in order to obtain the expert's product in a high quality and useful fashion. The selection and deployment of a particular expert or experts as part of the team will be critical judgments to make; integration of such experts into the team will be a management challenge. Outside assistance must be as carefully screened as participation of the police and prosecutors in the investigation. While close attention must be paid to the expert's special knowledge and skills, his true area of competence must be isolated and kept in mind. There must not be an unthinking or unquestioning deference to special knowledge to the detriment of objective fact-finding and professional evidence gathering. The overall conduct and direction of the investigation must remain firmly in the hands of law enforcement professionals. Each member of the interdisciplinary team has a valuable contribution to make and must be respected in these joint ventures as an equally contributing peer professional.

1.3.4 Utility of Outside Experts Assisting With Aspects of the Computer Related Crime Case

As was suggested in Section 1.2.1, computer related crime investigations and prosecutions are not always as exotic and exceedingly complex as many criminal justice practitioners believe. Certainly, from time to time, specialist consultants and expert witnesses will be required. But, in many ways, the requirements for the competent handling of a computer related crime case are not so very different than the requirements regarding assistance from experts with special knowledge in many other areas of white collar crime. Perhaps the main exception to this general rule is the probable requirement for more experts numerically, each relating to a highly specialized area of computer technology, when a total computer system may have to be analyzed, dissected and explained relative to a fraud scheme.

As was noted in Section 1.1.2, the methods employed by sophisticated computer felons to gain unauthorized access to computers, to alter computer programs, and to manipulate data going into, stored in or printed out of computers are new and complex, especially where financial crimes--fraud, embezzlement, etc.--are involved. New computer related occupations have arisen to supply trained personnel to perform the electronics and telecommunications engineering functions; to write computer programs in a wide range of mutually unintelligible programming languages; to plan and design computer networks; to operate computer hardware; to code and input data; to audit computer operations; to provide computer security; and to perform many other specialized functions. Not only are such job functions wholly separate, requiring different training and skills, but technologists proficient in the operation of one type or brand of hardware or software are often totally unfamiliar with others. Further, computer applications in one industry--for example, banking--are likely to be totally different from those in another--for example, real estate, or securities.

As we saw in Section 1.1.2, the type of computer crime perpetrated seems to be the key to the particular skills and job function of the perpetrator. A person skilled in any one of the above areas can commit a computer related crime, as can several specialists from different computer related disciplines working in collusion.

Depending on the nature and complexity of the case, investigors and prosecutors may have to call upon specialists from many of these different fields and select those who are directly familiar with the victim's operation and/or equipment, in order to prove a crime was committed, gather the evidence, determine modus operandi, identify the suspect(s) and assist in preparing the case for trial.

1.3.5 Caveats and Recognized Limitations on the Use of Outside Experts

Every public agency is facing severe budget pressures in the face of inflation, tax cut referendums and increasing citizen intolerance of wasteful public spending. With this in mind, agencies desiring to break some new ground in the area of computer crime must be both cost conscious and creative in managing their limited resources. It would be extremely embarrassing, to say the least, to pay an outside consultant a great deal of money for case assistance only to learn at a later time that people working in the requesting department had sufficient experience and background to have advised in the case development, and perhaps to have even done a better job than someone from the outside. Personnel bureaus and public agency training divisions should make a point of learning and documenting for future reference the depth and variety of the agency's human resources. Some systems are indexed and computerized, allowing retrieval by specialist skill areas, which may surprise those not presently utilizing such systems. It is maddening to search around frantically for an expert in foreign languages, computer systems, or documents examination only to find that he or she who works next door in your department, never volunteered the relevant information, or was never asked what unique skills they may have.

Concurrent with projected increased reliance upon expert assistance, there is also the potential for waste and abuse in the utilization of the expert's services. This must be recognized and minimized to the extent feasible. Needless to say, it would be extraordinarily embarrassing to have a special enforcement unit concentrating on criminal frauds and computer crime to themselves be ripped off or duped by a smooth talking consultant or expert. Such an investigation or prosecution unit enjoys a very high visibility in these types of cases--for good or bad results --and, consequently, must exercise an additional measure of care. On top of this hazard of public embarrassment and the resultant deterioration of public credibility, the negative fallout can be drastic during public budget hearings and internal resource allocation deliberations where an expensive expert has been managed ineffectively or has performed amateurishly. The paid professional expert will be required in many such cases. There is nothing wrong with this per se, assuming the responsible party can articulate why other available resources were not utilized or why they may have been inappropriate for a particular task or type of computer related crime case.

Not every computer related crime case will require extensive expert assistance, and for those that do, not every available expert will require compensation. As Chapter 2.0 points out, there exist sources through which the investigative agency can obtain outside technical assistance without cost. These should be explored first. When paid experts are used, law enforcement personnel must be careful to keep the cost of such adjunct services in reasonable proportion to the seriousness and complexity of the case.

Involving outside experts in a major crime investigative team so that they feel a part of the team and feel a commitment to the goals of the investigation is crucial. This must be balanced, however, against the need for security in the investigative unit, the fixing of responsibility and authority over the activities of the expert, strict management controls over the tasks the expert is to perform, and the need to keep overall control of the investigation in the hands of the investigator, not the outside expert. Later Chapters of this Manual will address these concerns in greater detail.

blank page

2.0 DEFINING THE EXPERT AND HIS OR HER ROLE

The term "expert" is widely used in the context of major case investigations, but connotations vary. This Chapter defines what we mean by "expert"; discusses various sources of experts and categories of experts based on their special skills; and gives an overview of the roles an expert can play in the successful investigation and prosecution of computer related crime.

2.1 "Expert" Defined

The Random House Dictionary of the English Language defines an expert as "a person who has special skill or knowledge in some particular field; specialist; "authority" or as a person "possessing special skill or knowledge; trained by practice; skillful or skilled (often followed by 'in' or 'at')."[1] Black's Law Dictionary defines an expert as one who is "a skillful or experienced person; a person having skill or experience, or peculiar knowledge on certain subjects, or in certain professions."[2]

The essential elements of both definitions are apropos to technical experts in complex criminal cases such as those involving computer related crimes. Experts are persons whose special skills, knowledge and/or training equips them to assist the investigative and prosecutive team with aspects of the case beyond the usual competence of law enforcement professionals. In this regard, the term "expert," as used throughout this Manual, is synonymous with "consultant" which is defined as "a person who gives professional or expert advice."[3]

Consonant with these terms is "technical adviser"--"adviser" being defined as "a person who gives advice" and "technical" as "peculiar to or characteristic of a particular art, science, profession, trade, etc."[4] The term "technical adviser" does not convey the strict notion of "specialness" that connotes an "expert". For our purposes, in most situations the terms are used interchangeably, though an employee of a firm which has been victimized by a computer crime could serve as a Government technical adviser to explain the details of his employer's operation without at the same time being considered an "expert" for any relevant purpose.

Finally, the term "specialist" has applicability here; it is defined as "a person who devotes himself to one subject or to one particular branch of a subject or pursuit."[5] "Specialist" conveys a narrower or more specialized skill than does "expert." Again, while the terms are generally interchangeable here, a computer programmer proficient in COBOL only and employed for the duration of his or her career in a single industry is probably more appropriately termed a "specialist" than an "expert."

2.1.1 Expert Witness Defined

While all expert witnesses who give testimony at trial are by definition accepted to be "experts" in their particular areas of competence, not all experts are expert witnesses. The role of the expert witness is an occasional and highly specialized utilization of a technical expert. Black's Law Dictionary variously defines an expert witness as, among other things, a "person competent to give expert testimony" and as a witness who has "acquired ability to deduce correct inferences from hypothetically stated facts, or from facts involving scientific or technical knowledge."[6]

2.1.2 Roles of Expert Consultant and Expert Witness Distinguished for the Purposes of This Manual

The term "expert" will, for the purposes of this Manual, refer to an individual who can, by virtue of knowledge or skill in any broad array of computer related professions, contribute that expertise in a manner which assists in the investigation or prosecution of a computer related crime. Although the term "expert" is commonly used interchangeably with the term "expert witness"--an individual who offers opinion testimony at trial--as we have seen this is a very restrictive application. For example, an individual who is employed by a law enforcement agency to provide pre-indictment investigatory assistance in a computer crime case should be considered an "expert," regardless of whether those services culminate in the presentation of opinion testimony at trial. The term "expert" is utilized here independent of the particular function an individual exhibits at any given point in the case proceedings. The term "expert" is more appropriately used to describe the special qualifications and skills which enable this individual to provide assistance in any particular phase of the computer related crime case.

2.2 Types of Expertise Distinguished by Source of Expert

As indicated above, the roles that can be assumed by an expert in a computer related crime case are variant, transitional and greatly influenced by individual case progression. Depending on the role which the investigative team foresees for an expert under a given set of facts and circumstances, one or more generic sorts of experts may be tapped. What follows identifies and describes each generic type of expert. Table 3 illustrates advantages and disadvantages in the use of each.

Table 3

Selected Expert Witness Sources
Advantages & Disadvantages

CATEGORY	POTENTIAL CHOICE	ADVANTAGE	DISADVANTAGE
Loaned Gov't Employee	-a system analyst from a gov't computer service bureau/ facility	-expert can be "loaned" to the prosecution team without cost	-generally not much choice as to particular expertise or personal qualifications -at trial, opposing counsel likely to challenge crediility by showing of bias or self-serving interest, i.e., job security
Retained Private Consultant	PAID--professional association, independent audit firm, or computer security organization	-allows selectivity in type of expertise and personal qualifications of individual employed	-at trial, opposing counsel likely to challenge by a showing of bias or pecuniary interest
	UNPAID--university or trade school	-no cost to employing party -generally objective and well qualified	-at trial, opposing counsel likely to challenge by showing self-serving interest; i.e., career advancement or organization promotion
"Provided" Victim Company	-Audit Department (EDP or internal)	-likely to be familiar with organization and system operations -often no cost to employing party	-at trial, opposing counsel likely to challenge by showing of bias or self-serving interest
"Provided" Computer Company	-computer manufacturing company	-often no cost to employing party -very familiar with systems operations and design	-may not want to reveal infallibilities of system which company manufactures
	-computer service organization	-likely to be very familiar with systems operations and security	-often reluctant to supply information concerning the vendor company; must maintain privacy and security of clients' data
Court Appointed	-gov't computer service bureau/facility -professional association -independent audit or security firm -university	-generally less biased -can be cross-examined by both parties in action	-may not always be the most prestigious or effective witness

2.2.1 The Confidential Informant/Technical Adviser

Under certain circumstances, confidential criminal informants or sources of information might conceivably be informally involved in the early stages of a criminal investigation as "confidential techical advisers." These individuals can be very helpful during an investigation for the purpose of interpreting events and developing undercover strategies or constructing hypotheses for the investigation of complex cases. Where this person has requested anonymity and protection, the investigator must anticipate the future, where a transition must take place from this type of informal technical assistance to a stage of "going public" with the informant's identity and preparing him to present evidence at trial and offer expert opinion testimony. With this possibility in mind, security considerations must be carefully weighed and a strategy for making such a transition thoroughly analyzed prior to engaging a confidential information source.

2.2.2 The "Loaned" Government Employee

The "loaned" Government employee as technical adviser is another potential source of expert assistance. This specialist may be loaned from another department in the agency conducting a computer related crime investigation or may be temporarily loaned from another agency of Government within the same geographical area.

A Government employee's objectivity, and consequently credibility, may be subject to attack on cross-examination on trial where it may be demonstrated the employee's job might be in jeopardy if a certain position was not adopted or where the defense can demonstrate a consistent record of testimony on behalf of one side on important issues. This may, under certain circumstances, work to lessen the utility of this type of consultant.

"Loaned" Government employees as experts can present management and control problems. Depending upon the egos and personality types involved, as well as the quality of leadership and supervision on the part of the requesting agency, a loaned employee expert may begin to sense a lack of tight management or knowledge by those he or she is assisting. If this happens, one of two results is probable. The expert may enjoy a brief vacation from regular duties and not accomplish much. On the other hand, if the expert is aggressive and conscientious and senses a vacuum, based upon superior knowledge and expertise, he may run away with the case. This may later create evidentiary and legal problems due to lack of expertise in investigation, creating hard feelings and adversely affecting future cooperative working relationships.

Both objectivity and control problems in the use of "loaned" Government employees detract from what is otherwise a reliable and cost-effective source of outside technical input. Care must be used in requesting the availability of such personnel.

2.2.3 The "Provided" Consultant

Private sector groups and organizations will often provide technical assistance without cost in the investigation of major criminal cases. Profit-making groups with an interest in the outcome of the case are frequently excellent sources of expert assistance. For example, the manufacturer or vendor of computer hardware or software that was violated by a computer criminal is likely to be the best source of technical information on the equipment's capabilities and vulnerabilities. Likewise, a manager and/or security specialist from the victimized firm are the best sources of needed information on the victim's operations, physical plant, high risk employees, etc. Likewise, some universities or trade schools and professional associations concerned with computer related crime might provide free technical assistance and support under conditions that would advance their private research interests in some way or enhance their public image in relation to some particular problem.

For law enforcement agencies which do not benefit from a sizeable budget for technical assistance, constructing such "win/win" working relationships are an excellent idea. In many respects, the most qualified and credible experts for a given purpose will be "provided" without charge from such sources. This can, of course, vary, but many universities and associations have resources with rich backgrounds in specialized field experience, current research, teaching, writing, consulting, and, very often, also in testifying in court. These types of resources exist in every jurisdiction, and they should be proactively identified and developed in relationship to areas of anticipated criminal investigative interest before they are actually needed. As has been documented in the past, very often the leading authority in a specialized field may find himself the object of a race by opposing counsel to employ his services. A good prosecutor and investigator team always wants their witnesses "locked in" early on in a case. However, this can raise the issue of the integrity and objectivity of the expert, if his or her predisposition toward a technical question may be that reliably predicted in advance.

The major caveat, of course, with regard to using employees of the victim corporation or computer supply vendors who have had dealings with the victim is that they are not necessarily above suspicion in at least the initial stages of the case.

2.2.4 The Retained Consultant

There is also the "professional expert" who is a consultant retained for a fee. It is wise to proceed with more than average caution in seeking to employ this category of expert assistance. Arguably, any person with sufficient resources and time can locate an equal number of qualified experts who will line up on any side of an issue that appears to correspond with the needs of the client. This is not to say, however, that all professional experts exhibit this tendency or that the consulting industry cannot be tapped to provide sound advice based on principle and experience. For example, independent, for-profit computer security consultants and EDP auditing firms who possess excellent reputations can be retained in cases where using the victim's personnel, or their peers from within the industry in question, is not advisable in a given case.

However, credibiilty (especially in terms of previous work advocating a contrary position), cost, objectivity and specific prior corporate experience are all factors that must be carefully weighed when deciding to retain a professional consultant.

2.2.5 The Court Appointed Expert

Court appointed experts are another possibility to be considered during the later stages of case disposition. This may be an attractive alternative or adjunct procedure under either of the following circumstances. First, the parties may not have sufficient resources or expertise to employ their own experts. Second, there may exist substantial disagreement by equally-qualified experts representing either side and their objectivity has come into question as a result of immersion in the adversary process.

Federal practice allows for the liberal use of court appointed experts. Rule 706 of the Federal Rules of Evidence provides as follows:

- Court appointed experts. (a) Appointment. - The court may on its own motion or on the motion of any party enter an order to show cause why expert witnesses should not be appointed, and may request the parties to submit nominations. The court may appoint any expert witnesses agreed upon by the parties, and may appoint expert witnesses of its own selection. An expert witness shall not be appointed by the court unless he consents to act. A witness so appointed shall be informed of his duties by the court in writing, a copy of which shall be filed with the clerk, or at a conference in which the parties shall have the opportunities to participate. A witness so appointed shall advise the parties of his findings, if any; his disposition may be taken by any party; and he may be called to testify under cross-examination by each party, including a party calling him as a witness.

- (b) Compensation. - Expert witnesses so appointed are entitled to reasonable compensation in whatever sum the court may allow. The compensation thus fixed is payable from funds which may be provided by law in criminal cases and civil actions and proceedings involving just compensation under the fifth amendment. In other civil actions and proceedings the compensation shall be paid by the parties in such proportion and at such times as the court directs, and thereafter charged in like manner as other costs.

- (c) Disclosure of appointment. - In the exercise of its discretion, the court may authorize disclosure to the jury of the fact that the court appointed the expert witness.

- (d) Parties' expert of own selection. - Nothing in this rule limits the parties in calling expert witnesses of their own selection.

2.3 Types of Expertise Distinguished by Subject Area Specialties

A wide range of technical specialists, each with differing expertise and job function, is involved in computer operations. Depending on the particular facts and circumstances of a given computer related crime case, any or all of these types of experts could be needed to provide technical assistance to the investigative and prosecutive team. Table 4 illustrates the range of such specialties; most job definitions are taken from the glossary of computer expertise provided in BJS' recent Computer Crime Criminal Justice Resource Manual.[7] The following sections describe the functional expertise of each type of expert and suggest areas for their optimal utilization.

TABLE 4

SELECTED COMPUTER RELATED OCCUPATIONS OF POSSIBLE EXPERTS

APPLICATIONS PROGRAMMER: One who designs, develops, debugs, installs, maintains, and documents applications programs.

COMMUNICATIONS ENGINEER/OPERATOR: One who operates communications equipment including concentrators, multiplexors, modems, and line switching units. Ordinarily, this person reconfigures the communications network when failures or overload situation occur.

COMPUTER CRIME SCHOLAR: A researcher, author or commentator on the problem of computer related crime, its causes and characteristics.

COMPUTER OPERATOR: A person who operates a computer, including duties of monitoring system activities, coordination of tasks, and the operation of equipment.

COMPUTER SCIENTIST: A person highly proficient in both electronics and programming, who usually holds advanced degrees in computer science. This person is generally not business-application oriented.

COMPUTER SECURITY SPECIALIST: A person who evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls that are related to the use of computer systems.

COMPUTER USER: A manager or professional staff member who is responsible for accomplishing the tasks for which computers are used. Generally, this person will interface with systems analysts and programmers who translate the users needs into computer production systems.

DATABASE ADMINISTRATOR: An individual with an overview of one or more databases, who controls the design and use of these databases. Responsibilities are the addition, modification, and deletion of records and frequently the security of the database.

DATA ENTRY AND UPDATE CLERK: A person who adds, changes, and deletes records in computer-sorted databases by means of computer terminal, or manually updates punch cards or entries on input data form for computer input.

EDP (Electronic Data Processing) AUDITOR: A person who performs operations, computer, computer program, and data file reviews to determine integrity, adequacy, performance, security, and compliance with organization and generally accepted policies, procedures, and standards. This person also may participate in design specification of applications to ensure adequacy of controls; performs data processing services for auditors.

FACILITIES ENGINEER: A person who inspects, adjusts, repairs, modifies, or replaces equipment supporting computer and terminal facilities, e.g., air conditioning, light, heat, power, and water.

JOB SETUP CLERK: A person who assembles jobs. This task includes compilation of data, computer programs, and job control information. This person requests that jobs be executed, requests media libraries for necessary data, physically places jobs and data into job queues, handles procedures for reruns, and possibly distributes output to users.

MEDIA LIBRARIAN: A person who files, retrieves, and accounts for off line storage of data on disk, tape, cards, or other removable data storage media. The person provides media for the production control and job set-up areas and functions, and cycles backup files through remote storage facilities.

OPERATIONS MANAGER: The manager of a computer facility responsible for the operation of the computer system. He may also be responsible for the maintenance, specification, acquisition, modification, and replacement of computer systems or computer programs.

PERIPHERAL EQUIPMENT OPERATOR: A person who operates devices peripheral to the computer that performs data input/output functions.

PROGRAMMER: A person who engages in designing, writing, and testing computer programs.

PROGRAMMING MANAGER: A person who manages computer programmers to design, develop and maintain computer programs.

SECURITY OFFICER: A person who evaluates, plans, implements, operates, and maintains physical, operations, procedural, personnel, and technical safeguards and controls.

SYSTEMS ANALYST: A person who engages in system requirements, specifications, and design activities. This person specializes in applications and performing systems analysis, and generally works independently from the computer user and programmer.

SYSTEMS ENGINEER: A person who designs, configures, tests, diagnoses, assembles and disassembles, and repairs or replaces computer system devices and components.

SYSTEMS PROGRAMMER: A person who designs, develops, installs, modifies, documents, and maintains operating system and utility programs.

TECHNICAL ENGINEER: A person who tests, diagnoses, assembles and disassembles, repairs, and replaces terminals or their components.

TRANSACTION OPERATOR: A person who operates a computer transaction terminal by entering transactions for processing by a comuter system.

2.3.1 General Experts

Several categories of overall experts are not specifically involved in the operation of particular computer systems or services. Their expertise is more general but still useful, especially when providing background orientations for the investigative team or overviews for a judge or jury. Such "general" experts include the following.

2.3.1.1 Computer scientists

The computer scientist is a highly-trained and specialized computer technologist whose areas of competence cover both the electronics engineering and progamming aspects of computers. Because they tend not to be on the staff of victim companies and their focus is on broad computer planning and design considerations, they tend not to be familiar with specific business applications of computer technology.

2.3.1.2 Computer related crime researchers and scholars

A growing number of social scientists and legal practitioners have researched both individual computer crimes and the phenomenon in general. Their works are being increasingly published and cited. In addition, many such experts have served as computer related crime training instructors and lecturers before law enforcement groups and others, and many have testified before Congress and State legislatures on the problem of computer crime and on the advisability of pending computer related crime legislation. Such experts could be effectively employed at several key junctures in a computer related crime case. Providing background orientation to the newly-assembled investigative team, helping to "profile" likely suspect types once the case gets underway, and providing useful expert testimony on the varieties of reported computer related crimes and criminals are three such applications. Under certain circumstances, and budgetary constraints allowing, such scholars could serve as senior technical advisers throughout the course of a major computer related crime case.

2.3.2 Subject Matter Experts from Various Data Provider and Computer User Communities

The nature of a computer related crime will vary greatly from one victimized industry to another, and within a given industry. To cite an example, banking applications for computer technology differ from real estate applications and both differ from hospital services applications. Computerized payroll and accounting functions within a given industry, to take another example, will vary between two businesses.

Data providers are generally clerical and administrative personnel who generate and process manually prepared data destined for input into a computer or who keypunch (code) such data for actual input. Their particular functions and levels of competence will vary widely and depend on the industry in which they work and the procedures at a particular employee's operation.

Data providers have considerable opportunity to mishandle, alter or otherwise manipulate data before it is fed into the computer and, again, once it is printed out. Because data providers are often involved in the perpetration of computer related crimes, they can prove useful during both the investigative stage and at trial, as expert witnesses, to explain routine data processing procedures at the victim's business, and to authenticate certain non-computerized records such as data coding sheets or printouts, etc.

Computer users tend to be business managers and other professional level staff who rely on computer applications, and computer-generated data, to perform their jobs. Generally, they interface with computer analysts and programmers within their organizations, on whom they depend. However, with the advent of microcomputers, such personnel are themselves increasingly operating computers and performing relatively simple business and technical functions. Computer users include the following categories of personnel:

- business executives,
- bankers,
- stock brokers,
- medical technicians,
- accountants,
- personnel management specialists, and
- internal auditors.

The list of computer users is virtually endless.

The utility of computer users as experts in part parallels that of data providers. Because of their high level of responsibilities and competence, they can be used to provide even broader insights into the victim corporation's general operations, personnel functions, computer applications and other details. Such persons are also often in sensitive positions which allow them to suggest the identities, motives and modus operandi of potential suspects.

2.3.3 Computer Technologists

There exist major divisions between computer technologists, both because some are skilled in electronics aspects and others in programming, and because some are proficient at business applications of computer technology while others have specialized in research applications, etc. Understanding the distinctions between the major technologist professions is an important first step toward understanding their comparative utility as experts and expert witnesses.

2.3.3.1 Electronics engineers

These persons, whose backgrounds are in electronics, are skilled at designing and repairing the electronic circuitry of computers. Their familiarity will often be limited to computer hardware of particular make or manufacture.

2.3.3.2 Telecommunications engineers

These specialists are responsible for the interface between and among computers. They create computer networks through "front end" hook ups of remote terminals to computers located elsewhere by means of telephone switching systems. They maintain the satellites, cables and other devices which are the connectors between two or more computers in a computer network.

Like EDP engineers, telecommunications engineers may be useful as experts in complex computer fraud cases. Especially in the area of EFTS, input from telecommunications experts as to how a vast computer network operates can be important at the investigative, pretrial and trial stages.

Because of the nature of their function, telecommunications engineers are not generally on the staff of a single computer user organization which is the victim of a computer related crime. Telecommunications equipment manufacturers and engineers constitute wholly separate industries. Their familiarity with the user applications of a single victim organization may therefore be extremely limited. On the other hand, where whole computer networks have been victimized, the telecommunications engineer can play an important role in successful investigations.

2.3.3.3 EDP programmers

These technologists design, write, and test computer programs, for business and other applications. Generally this is a staff function in a business operation, where individual programmers interface with managers and computer users in the day-to-day implementation of computer applications to business problems.

Obviously the programmer who wrote a particular computer program that was altered or is otherwise involved in a computer related crime is the best expert to employ for identifying, interpreting, and authenticating the evidence--unless he or she is a suspect. Disadvantages from the use of the victim organization's in-house programmers as an expert extend also to the fact that their familiarity with a wide range of computer applications within the oranization may be limited. Care must also be exercised in using outside programmers as experts due to the fact that individual programmers proficient in one programming language or manufacturer's make of software are frequently unfamiliar with others.

2.3.3.4 Systems analysts

Systems analysts design computer system applications to meet user requirements and specifications. They may or may not themselves be programmers, but are regardless at a high level of responsibility within an organization. The utility of having the victim organization's systems analyst serve as an expert derives from his or her familiarity with both the user needs and specifications and the programming applications within the organization. Using systems analysts not directly familiar with the victim's equipment, programs and user applications can run into the same problems noted above for computer programmers.

2.3.3.5 Database managers

With the increased volume of stored computerized data in large organizations, information systems specialists called "database managers" have been added to staff. These individuals are responsible for the overall administration of the organization's data storage and retrieval capability, both with regard to information stored in the computer itself and on magnetic tapes and other software kept in libraries or other storage areas. A computer criminal's tampering with an organization's computerized data can run the gamut of complexity from erasing or sabotaging a secured magnetic tape, to applying highly sophisticated surreptitious techniques to scan computer-stored data for espionage purposes or alter it in furtherance of a fraud scheme.

Use of the victim's database manager as an expert to assist the investigative team to determine a computer criminal's modus operandi could be critical. Likewise, calling the database manager as an expert witness to testify to the victim's standard procedures for data storage and retrieval, as well as to indicate chain of custody for key computerized records, can be important at trial.

2.3.4 EDP Auditors

Auditors are key technical advisers in the investigation and prosecution of any complex financial crime. EDP auditors are a highly specialized subgroup of the audit community, as they do not generally follow a "paper trail" as do other auditors. (For an overview of the special tools and techniques used by EDP auditors, see Appendix "E" to BJS' Computer Crime Criminal Justice Resource Manual.[7]) However, with this exception their role and function parallels those of other auditors, in that they review data files to determine their integrity, adequacy, security, and compliance with an organization's internal policies and standards and with the generally-accepted norms of computerized record-keeping.

EDP auditors are generally on staff in the internal audit departments of large organizations. Others function independently, or as part of audit organizations--external EDP auditors.

Because of their independence, level of technical expertise, and the rigors of their profession, EDP auditors can serve as key technical advisers and expert witnesses on a whole range of issues in the case. The adversarial relationship between many auditors and the audited units within an organization, as well as the fact that the internal EDP auditor is in a sensitive and high risk position with regard to perpetrating such crimes, may argue against using the victim company's internal EDP auditor(s).

2.3.5 Computer Security Specialists

These individuals are responsible for any or all aspects of physical plant security, protection of personnel and hardware, and data security (software, etc.). Many are computer technologists whose primary concern is data security. Others are industrial security specialists, with or without criminal justice background or training. Depending on the size, nature and scope of its operations, a victim organization provides more or less computer security for its physical plant, hardware and software, and personnel. The facts and circumstances of the case will dictate whether, and if so, how, the victim organization's computer security staff should be utilized as experts. As in the case with the internal EDP auditor, the internal computer security specialist is in a position of trust and controls considerable access to facilities and operations. This makes the internal co puter security specialist a high risk candidate for committing computer related crime and may argue for retention of an outsid computer security consultant.

Computer security specialists can be especially helpful at understanding the victim's operations, at crime scene search, at obtaining evidence, and at assisting in the identification of suspects. These and other functions make him or her a potentially important expert at the investigative, pretrial, and tria stages.

2.3.6 Hardware and Software Manufacturers and/or Vendors

The production of computer hardware and software is a large and growing industry. The manufacturers and vendors of th equipment in use by a victimized organization are perhaps the most qualified and reliable sources of information on equipment capabilities, applications and vulnerabilities. Often their representatives will volunteer technical assistance without cost out of a public service commitment and/or to counter the negativ impact of having their equipment successfully violated in the course of a computer related crime. So long as they provide employees who are experienced in the applications of their equipment in the victimized organization, this source of expert can b extremely important throughout the investigative, pretrial and trial stages.

2.3.7 Computer Service Representatives

Many organizations contract out for a variety of computer services and functions. The computer service industry, like the computer hardware and software manufacturing industries is a large and diversified one. Services extend from providing keypunch services to time sharing on remote computers, from deve opment for sale of pre-packaged computer programs to offering specialized data processing services.

Often outside computer services have been utilized by a victimized organization. Because the computer service industry is highly competitive and their representatives have regular access to their customers' data there is a high risk of computer crime among this group. The fact that computer service representative may, at least initially, be among the prime suspects in a computer crime case lessens their reliability as technical advisers. However, the assistance of particular computer service organizations to establish modus operandi, isolate suspects, and assist in the evidence interpretation and authentication stages is often critical.

2.3.8 Experienced Computer Related Crime Investigators and Prosecutors

Public and private sector investigators who have had direct prior experience in the investigation and prosecution of computer related crimes are valuable technical advisers at all stages of the case. Where these experts are not already on the staff of the law enforcement agency handling the case, their services may be obtained by loan from another agency or, in the case of many private sector investigators, for a fee. Perhaps the largest single disadvantage of bringing an experienced outside investigator or prosecutor into the team is the danger that he or she will attempt to take over the management and direction of the case.

2.3.9 Forensic Scientists

As with other kinds of criminal cases, authentication of physical evidence will require the performance of certain tests and other procedures. The forensic scientist plays an important role in any computer related crime case where computer software, printouts or other physical evidence is at issue, whether or not such items are ever introduced formally into evidence at trial. Thus, forensic scientists constitute an important group of technical experts to be called upon at the investigative, pretrial, and trial stages of the case.

As in the case with forensic experts in other major cases, their services may be obtained in-house, via "loaned" or "provided" arrangements with other agencies or organizations, or for a fee depending on local circumstances.

2.3.9.1 Forensic chemists

Issues of authentication can arise when attempting to determine the origins of magnetic tapes, printouts and other computer related tangible evidence. In addition, proving or disproving that a particular magnetic tape has been altered, for example, can be an important evidentiary issue in a computer related crime case. Forensic chemists will be required to perform such tests and to testify at trial to their findings.

2.3.9.2 Document examiners

Determining the authenticity of computer related records can be an important evidentiary issue in a computer crime case, as in other criminal cases. For example, determining from which computer printer a particular printout came, or that two or more printouts were generated by the same or different machines, can be a central issue of fact. In this regard, expert document examiners are key technical advisers at all stages of the case.

2.4 Summary Overview of the Role of the Expert in A Computer Related Crime Case

The role an expert will assume in a computer related crime case will depend on a number of interrelated factors such as the specific nature of the crime, the environment in which the crime was perpetrated, and the organizational structure of the law enforcement agency which is controlling the investigation or prosecution. Additionally, the role of the expert may frequently be multifaceted and transitional. For example, an EDP auditor who is employed during the investigatory phase of a case to analyze computer-generated records may later be called upon to testify at trial as to the validity and reliability of the questioned data. This same expert may function as an adviser to the primary investigator in interpreting the findings of the audit and, later, as an assistant to the prosecutor in translating the finding into a foundation for competent and successful evidence presentation.

The role of an expert in a computer related crime case, although potentially quite variant, is always aimed at assisting in the overall effort of the investigative or prosecutorial team. Very few if any law enforcement agencies have sufficient resources available to train investigative staff in such a highly-diversifi and progressive technical field. Even in police departments which have a specially-designated economic crime unit, the need for certain types of computer related expertise may be evidenced. It is unreasonable to expect that all technical assistance requirements on a complex computer crime case can be met by in-house staff, however well-qualified these individuals may be.

The computer expert brings to the investigative or prosecutive team specialized knowledge, training and/or experience which serves to strengthen the pre-existing information/skill level of the team. The degree to which a particular expert becomes involved in a case essentially depends on the case-specific technical assistance requirements identified by the team manager. The depth of a given expert's involvement will frequently increase as the case develops and as more complex technical issues arise.

3.0 WHEN TO EMPLOY AN EXPERT

As noted in Section 1.1, computer related crimes are not homogeneous. To the contrary, a wide variety of criminal acts fall within this domain. While a variety of definitions have been posed for what constitutes a computer related crime, as we have seen, this Manual adheres to a broad definition of the term. Consequently, the question of when to employ an expert, or experts, in a computer related crime investigation or prosecution will vary significantly. The following sections discuss the primary factors likely to dictate when to look for outside expertise in such cases.

3.1 Computer Related Crime Cases Vary Greatly in Complexity and Type

As was discussed in Section 1.1, "computer related crime" is a term which can be applied to the whole spectrum of illegal activities in which the computer is the object, the subject or the instrument of the crime, or in which the symbolic presence of the computer can be used to intimidate or deceive the victim. Such cases will run the gamut from the least to the most complex for investigators and prosecutors themselves to understand and for purposes of obtaining a conviction at trial. Case type and complexity will be the primary factors bearing upon the questions of whether, and if so, when, to bring outside experts into the case.

3.1.1 Need for Technical Assistance Will Depend on Case Type, Complexity

The less complex and involved the case under analysis, the further in-house staff can proceed without specialized outside advice or assistance. Even absent a basic understanding of computer systems and operations, the investigative team will often be immediately qualified to confront many computer related crime situations where the computer has been the object of a criminal attack in the form of physical sabotage. The requirements of such cases may not be significantly different than other "routine" investigations involving crime scene processing, preserving the evidence, disarming and apprehending the suspect, interviewing witnesses, estimating the damages, etc.

This situation would be in sharp contrast with the skill requirements needed to conduct an investigation of an ongoing financial swindle by means of computer, perpetrated by unknown individuals, where merchandise inventories are being unlawfully diverted to fictituous businesses through the illicit entry into and manipulation of a corporate conglomerate's complex computer network spanning many States, or even countries. The contrasting level of complexity of such cases is readily apparent from their earliest stages. However, consider this possible scenario: While conducting an apparently "routine" investigation of physical sabotage against a computer's software, leads surface from interviewing employees of the victim company which suggest that other employees perpetrated the act in a deliberate effort to conceal an ongoing data manipulation scheme. In this instance, although there was no apparent need to seek outside expert assistance in investigation of the physical attack, further inspection has revealed more complex motives requiring an in-depth investigation, which will necessitate both a sophisticated understanding of computer operations and a knowledge of the victim company's operations.

A re-evaluation of the need for outside expert assistance obviously will be necessary in this situation to compensate for unforeseen case developments. Pre-existing staff resources and capabilities may need to be reinforced by the addition to the team of one or more outside experts who have extensive experience with the operations of the particular computer system in question. In a routine criminal investigation involving physical damage to a computer system, the potential for uncovering evidence or information which is indicative of more extensive foulplay always exists. Therefore, with this possibility in mind, it is important to consider seeking the services of a computer expert from the onset of the investigation. Data manipulation might go undetected in a routine criminal investigation of this sort, which by its nature will tend to focus more on readily apparent physical evidence of computer abuse, rather than on more complex motives or the possibility of perpetrating one crime in order to conceal another, more serious one.

A preliminary investigation to determine the scope of such an apparently simple crime could be conducted by in-house staff, provided a certain degree of familiarity with computers exists. If this investigation leads to evidence of a significantly more complex nature, then it will probably be necessary to employ an outside expert (providing the agency does not have a resident computer specialist) who can conduct a thorough analysis of the situation and provide the in-house team with the degree of technical input required to pursue the investigation on a well-informed basis.

Table 5 illustrates the likelihood of needing outside technical assistance at the various key stages of a computer related crime case. The comparative need for outside expertise at each stage will vary with the types of computer related crimes, as discussed earlier in Section 1.0. Table 5 addresses this aspect of the problem, as well.

TABLE 5

KEY PHASES OF COMPUTER RELATED CRIME CASES LIKELY TO REQUIRE EXPERT ASSISTANCE BY GENERAL TYPE OF CASE AND LEVEL OF ASSISTANCE NEEDED

KEY 0: No Expert Assistance Required. 1: Need for Expert Assistance Remote. 2: Expert Assistance Likely to be Useful. 3: Expert Assistance Likely Necessary.	Malicious Destruction of Computer Hardware, Software	Industrial Sabotage, Espionage, Extortion, Terrorism by Computer	Defrauding the Public Through Symbolic Imagery by Computer	Complex Financial Crimes Against Business by Computer	Diversion and Theft of Non-Liquid Assets by Computer	Unauthorized use of Computer by Employees for Private (illicit) Purposes
Understanding Basics of Computer Processing	0	3	1	3	3	2
Advising on Sound Case Preparation and Trial Techniques	0	3	1	3	3	2
Understanding Patterns of Computer Abuse in Given Industry	0	3	2	3	3	2
Profiling Computer Felon	1	3	0	3	3	2
Detecting the Complex Computer Related Crime	0	2	0	3	3	2
Understanding Victim Company's Operations	1	3	0	3	3	2
Understanding Victim's Hardware, Software and Its Application	1	3	0	3	3	3
Preparing Search Warrants, Subpoenas	0	2	2	3	3	3
Crime Scene Assistance	1	3	0	3	3	2
Obtaining and Preserving the Evidence	1	3	2	3	3	3
Interviewing and Interrogating Witnesses	0	3	1	3	3	2
Interpreting the Evidence	1	2	1	3	3	2
Focusing the Investigation on a Suspect	1	2	0	3	3	2
Determining Modus Operandi	0	2	1	3	3	2
Anticipating Defense Objections	0	2	2	3	3	2
Preparing the Case for Trial; Pretrial Discovery	0	2	2	3	3	2
Getting the Evidence Admitted	0	3	3	3	3	3
Advising on Cross Examination of Defense Experts	1	2	1	3	3	2
Making Technical Presentations to Jury, Judge	0	3	2	3	3	3

3.1.2 Number and Type of Experts Needed Will Depend on Case Type and Complexity

As noted in Section 2.3, the rise of computer technology has given birth to a variety of new special fields, which in and of themselves constitute separate professions. In addition, the proliferation of the computer hardware and software manufacturing, vending and service industries has resulted in computer technologists specializing in working with only certain programming languages (e.g., FORTRAN, COBOL, SPSS, BASIC, etc.) and in working with only various makes and models of equipment. To complicate matters further, the operational applications of computer technology will differ substantially from one industry to another (e.g. banking versus real estate) and for different activities within a given industry (e.g. accountants, personnel managers). The day-to-day operations of two competitors in a given industry may also differ markedly, resulting in very different situations with regard to computer physical security, equipment configurations, opportunity and motive of suspects, etc. for each such corporation.

Each of these factors will have more or less of a bearing on a computer related crime case, depending on the nature and circumstances of the case. However, as a rule of thumb, the more relevant the above factors, the more complex the case, the more likely will be the need for multiple outside experts, each with his or her own specialization. Table 6 illustrates some of the types of experts likely to be useful at possible stages of computer related crime cases, not all of which will be present in every case. These likely types of experts to be used at various stages include the following:

- computer scientists;
- electronics and telecommunications engineers;
- computer related crime researchers and scholars;
- subject area experts from the victimized industry (e.g. bankers, stock brokers);
- computer users (i.e., managers) from the victim organization;
- computer technologists in the employ of the victim, including:
    - EDP programmers,
    - systems analysts, and
    - database managers;

- computer technologists external to the victim organization, but of the above same types;
- internal and external EDP auditors;
- internal and external computer security specialists, including;
  - database security specialists, and
  - physical security specialists;
- computer operators and data providers employed by or who interface with the victim organization;
- hardware (HW) and software (SW) manufacturers, vendors and computer service representatives associated with the victim's equipment;
- forensic scientists, including;
  - forensic chemists, and
  - document examiners; and
- investigators and prosecutors experienced at CRC cases.

For a detailed description of the functions of these experts, see Section 2.3, above.

3.2 Philosophy and Capabilities of the Law Enforcement Agency Will Impact on the Use of Expert Assistance

While the nature and complexity of a given computer related crime case will bear most directly on whether and when the investigative team will need outside technical assistance, the peculiar features of the agency itself will also have a bearing. Obviously, a large urban police department with specialization among its detectives, resident forensic scientists and in-house computer specialists operating EDP functions within the department itself will be in a much better position to successfully investigate such cases without resort to outside experts than would a rural sheriff's department or small town police force. A State-wide department of law enforcement or a specialized white collar crime strike force would likely be even better equipped with in-house resources which could be brought to bear than would the average big city police department.

However, apart from its size and manpower, the law enforcement agency's crime fighting philosophy will also have a significant bearing on its capability to react to such crimes. Considering the three generally available approaches to the successful investigation and prosecution of computer related crime--reactive, proactive and a combination of the two--the agency's method of operation will, to a large extent, determine when expert assistance is sought and intelligently employed. Finally, the quality and preparedness of agency human resources will be a reliable indicator of when to yell for outside professional help.

3.2.1 The Reactive Approach to Law Enforcement

Many police departments and prosecutor's offices continue to operate according to a strictly complaint-oriented approach. Regardless of their level of success in solving crimes and obtaining convictions, such agencies have retained a "reactive" philosophy of crime fighting. Staffing complements and specializations, agency budgets and standard operating procedures will generally reflect not only the complaint-oriented approach to casework but will also tend to be strongly reflective of the traditional sorts of cases which have over the years formed the bulk of the agency's workload.

Such departments operate under several constraints when faced with the increasing prevalence of computer related crime. First, because such crimes are often difficult to detect and are notoriously underreported, waiting for criminal complaints to be filed in such cases will have very limited impact on the problem of computer related crime in the jurisdiction.

Few such cases are likely to come to the attention of law enforcement through this route. Consequently, the capabilities and "front line" experience of in-house staff--investigators, prosecutors and specialist staff--in responding to such cases will tend to be underdeveloped and a greater reliance on outside expertise at all stages of those computer related crime cases which do get filed will likely be required. Because the "reactive" agency's investigative procedures will tend to be more routine and traditional, the points at which such outside expert assistance will be needed will also tend to be more predictable.

Finally, because of the infrequency of such cases coming to their attention through formal complaints, such reactive law enforcement agencies will not likely have developed regular procedures for calling in the necessary outside experts nor have established referral sources. The victim organization or complainant will probably exercise the initiative in suggesting when outside expertise is needed and who should be called into the case. There are obvious disadvantages that accrue from being in this posture when commencing the investigation of a complex financial swindle or other white collar crime case.

3.2.2 The Proactive Approach

Other criminal investigative and prosecutive agencies have developed a more "proactive" approach to major crimes investigations, especially in the white collar crime area. Such units initiate major investigations into pre-targeted activities and industries in their jurisdictions, which entail a high risk of fraud, embezzlement, etc. Such agencies do not necessarily wait for formal complaints to be filed in order to begin to investigate possible abuses. They appreciate the effectiveness and potential pay-off of crime prevention, criminal intelligence gathering, and crime deterrence activities which are ongoing and not dependent upon the filing of a complaint but which at the same time can uncover lucrative, illegal activities and generate high level, successful prosecutions.

Obviously, the existence of such units requires the support of the taxpayers and policymakers in their respective locales. They must also display dynamic leadership, a sophisticated approach to the internal management of major crime investigations, a strong sense of organizational mission, adequate resources, and highly-motivated and trained staff. The absence of any of these ingredients can render the proactive approach to crime fighting ineffective.

Clearly, no law enforcement agency can operate entirely in the proactive mode. All must also operate reactively, i.e., respond to particular filings. But for those agencies which have made a major commitment to include proactive (i.e. self-initiating) investigative efforts in their crime fighting strategy, there are two types of proactive operations that can be undertaken--poorly-informed and well-informed. Well-informed action requires a sophisticated criminal intelligence capability which can collect, collate, analyze, and evaluate field data, then plan and execute concerted tactical and strategic responses through the use of multidisciplinary major crime teams.

Technical experts, if affordable and available, can be very helpful at each stage of this process, especially in the intelligence gathering, analysis and evaluation stage and at the planning stage. Because such casework in its early stages is much more akin to applied research than it is to the traditional law enforcement roles of making apprehensions and obtaining convictions of particular individuals, proactive law enforcement agents must have a strong sense of internal discipline and a philosophical commitment to such activities as being a legitimate part of the police and prosecutive functions. They must identify and mobilize sources of expertise outside their units which can be tapped as needed, and develop ongoing working relationships with various key types of technical advisers, e.g. EDP auditors, computer security specialists, and experienced investigators from other units or jurisdictions who can be called into such cases at the preliminary stages.

3.3 Look First to In-House Resources

As we have seen, not all computer related crimes are complex, nor do they all require an in-depth knowledge of computer technology for their successful resolution. Many of these less complex cases can be solved with traditional investigative resources. Even for those computer related crimes of a more complex nature, expertise may well exist in-house that can be identified and brought to bear without turning to outside resources, whether paid or donated.

To a very large extent, the need to seek outside assistance will be determined by the resources and capabilities of the investigative or prosecutive agency. Whether available capabilities and resources can meet the demands of the case depends, as we have noted, essentially on the level of case complexity. When considered together, these two factors determine both the type of skills and experience needed, and the direction and depth of the investigative/prosecutive effort. The most effective and efficient method of utilizing in-house resources and capabilities is to identify and document their availability on a continuing basis. In order to be well-informed and well-prepared, an organization must make a point of identifying and referring its resources and capabilities in a readily accessible manner. Many agencies have developed computerized information retrieval systems which index personnel on the basis of special areas of knowledge and expertise. Much time and effort can be saved in the long run by proactively identifying potential in-house resources and capabilities, not to mention the financial savings that can be realized from using in-house personnel rather than paid consultants.

As investigative or prosecutive agency can identify a pool of in-house technical experts in the computer abuse area, as in other subject areas, prior to case demands, but in some instances it can be expected that the nature of the case will be such that it requires extensive knowledge and experience in a very specific facet of computer technology or computer applications--a background which may not be evidenced by any of the previously identified in-house experts. Other cases may require a great diversity of specialized skills, often not equally or sufficiently represented by the identified in-house resource pool. No organization can reasonably expect to fill all of its expert assistance requirements with strictly in-house staff. When a clear need for assistance has been demonstrated and there is a lack of in-house capability or availability, the process of selecting an outside expert can and should begin.

Attendance at specialized training courses and a review of other computer related educational materials can significantly aid in extending an agency's range of in-house investigative or prosecutive skills, especially where the investigation or prosecution centers around a relatively non-complex form of computer related crime. Even when the crime is of a sophisticated nature, previous educational exposure to the subject will provide in-house staff with a decided advantage in not only recognizing the scope of the problem, but in knowing what type of supplemental expertise is needed and where to find it.

3.4 Factors That Will Determine Whether and Where to Turn for Outside Expert Assistance

A wide variety of factors will influence the decision of when and where to turn for outside technical assistance in a given case, should in-house resources prove nonexistent or inadequate. Some of these factors will be dictated by the peculiar facts and circumstances of individual cases, and are thus not generalizable. However, several key factors of a generic nature will be relevant considerations in all cases. This section presents an overview of those key factors.

3.4.1 Nature and Complexity of the Case

As noted in Section 3.1, computer related crime cases vary greatly in complexity and display differing typologies. In addition, case complexity is the single greatest factor that will determine the extent of technical assistance needed in the case. As Table 5 illustrates, certain kinds of computer related crime cases will invariably require outside expertise, other kinds of cases, less so. Table 6 goes on to suggest the sorts of experts likely to be needed at each major stage of complex computer related crime cases.

3.4.2 Case Sensitivity

Computer related crime cases can run the gamut in terms of displaying sensitive aspects or involving prominent suspects. The presence of such factors can be expected to have a major impact when and where to involve outside experts in the case. Complex financial swindles or diversion of business assets by computer can, if they become known to corporate stockholders or to the general public, precipitate a crisis in confidence for the victimized business, having repercussions for sales, investment prospects, etc. Espionage or extortion or acts of political terrorism by computer can, if they become known, also impact on the perceived stability of the public and private sector organi-

Table 6

Some Possible Types of Experts to be Utilized at Key Points in a Computer Related Crime Case

Understanding Basics of Computer Processing	Computer scientist; programmer/systems analyst; external EDP auditor; subject area experts; CRC researcher/scholar.
Advising on Sound Case Preparation and Trial Techniques	Experienced CRC investigator; forensic scientist; CRC researcher/scholar, EDP auditor; computer security specialists.
Understanding Patterns of Computer Abuse in Given Industry	HW/SW manufacturer/vendor computer services rep.; subject area experts; computer users; external EDP auditor; experienced CRC investigator; CRC researcher/scholar.
Profiling Computer Felon	Systems analyst; EDP auditor; security specialist; HW/SW manufacturer/vendor; computer users; CRC researcher.
Detecting the Complex Computer Related Crime	Internal/external EDP auditors; database mgr; computer users; internal/external computer security specialists; experienced CRC investigator; CRC researcher/scholar.
Understanding Victim's Operations	Internal EDP auditor/computer security specialist/programmer/systems analyst/database mgr.; computer users/operators; data providers; subject area experts.
Understanding Victim's Hardware, Software and Its Applications	HW/SW manufacturer/vendor; computer services rep.; computer users; computer operators; data providers in-house programmer/analyst; internal EDP auditor; database mgr.
Preparing Search Warrants, Subpoenas	Internal/external systems analyst/EDP auditor/electronics enginee subject area experts; computer users/data providers; experienced CRC investigator.
Crime Scene Assistance	Programmer/systems analyst; database mgr.; computer users/operators; data providers; forensic scientists; computer security specialist; experienced CRC investigator.
Obtaining and Preserving the Evidence	Internal/external EDP auditors/programmers/systems analysts/computer security specialists; forensic scientists, experienced CRC investigators.
Interviewing and Interrogating Witnesses	Computer users/operators; data providers; internal and external EDP auditors; experienced CRC investigator; internal/external computer security specialist.
Interpreting the Evidence	Any or all of the above types of experts.
Focusing the Investigation on a Suspect	Internal EDP auditors/systems analysts/computer security specialists; computer users and subject area experts, experienced CRC investigators.
Determining Modus Operandi	Any or all of the above types of experts.
Anticipating Defense Objections	External EDP auditors/computer security specialists; experienced CRC investigators; CRC researchers/scholars.
Preparing the Case for Trial; Pretrial Discovery	Any or all of the above types of experts.
Getting the Evidence Admitted	Any or all of the above, as to laying the foundation, chain of custody, authentication, expert opinion, etc.
Advising on Cross Examination of Defense Experts	Any or all of above types of experts.
Making Technical Presentations to Jury, Judge	Any or all of above types of experts.

zations so victimized. The possible involvement of organized crime figures, public officials and/or top level corporate managers in the perpetration of complex computer related crimes can also attach a special degree of sensitivity to the case at the investigative stage.

Such factors, depending on the individual case at hand, may make it more or less advisable to seek outside technical assistance. The presence of such factors may drive up the stakes for the successful breaking of such a case to the point where greatly increased outside resources are called in, despite cost considerations. On the other hand, the stakes may well dictate that no outsiders--or, at least, outsiders with whom the law enforcement agency has not worked closely on previous cases--be called in. Very often such considerations will also dictate the use of outside experts from certain sources (for example, the victim organization or private sector paid consultants).

The trade-offs that will be encountered when deciding whether and when to use outside experts in especially sensitive computer crime cases are apparent and real. The presence of such factors should not, however, automatically dictate the non-use of outside advisers. Obviously, most computer related crime cases are comparatively sensitive. At the same time, most, as has been seen above, can be expected to require outside technical assistance to some degree. Section 5.0 discusses in detail the privacy and security considerations that are inherent in most computer related crime cases, and suggests techniques for insuring the security and integrity of the investigation.

3.4.3 Previous Experience With the Use of Experts

As is recommended at other points in this Manual, law enforcement agencies are urged to develop ongoing relationships with organizations which can supply experts as they are needed, and to preserve relationships with key individuals used in previous cases whose performance as experts was satisfactory or better. The advantages to using individual advisers already familiar with the agency and, ideally, with the investigative members of the team, are readily apparent. These considerations are discussed later in Chapter 7.0. Sources of experts with whom arrangements can--and should--be made to preserve their general availability are discussed in Section 4.5, below.

Previous experience at using experts in computer related crime cases will not only suggest to whom to turn but will provide important experiential input for deciding at what point, for how long, and for what range of tasks a given type of expert should be called in. The overall management and budgeting of the present investigation will greatly benefit from such previous experience.

For the law enforcement agency which has not had previous experience with computer related crime cases, valuable insights can be obtained from contacting neighboring departments or other organizations with which the agency interfaces to access previou experiences in this area as an aid to deciding whether and when to call in outside help.

3.4.4 Fiscal and Budgetary Considerations

Accessing outside technical assistance for a major crime investigation *can* prove very expensive, though by no mean are high costs for consulting fees inevitable. Sections 4.1 and 4.5, below, address the questions of comparative costs of variou types of experts and the sources of such experts, which will hav a direct bearing on cost. For our purposes here, suffice to say that the apparent complexity and expected duration of a computer related crime case may have major implications on the cost of outside technical assistance. Cost considerations in long, complex investigations may not only dictate turning to other public agencies, the victimized organization, or other private sector businesses for the no-cost services of experts rather than utilizing experts who will charge a fee but may also dictate bringing fewer experts into the case, bringing them in late in the case, or--if gratis technical assistance proves unavailable--not bringing outside experts in at all.

Obviously, a whole range of factors such as comparative importance of the investigation, size of the agency or unit budget, and strength of the case will be taken into initial consideration--and periodic reconsideration--when investigating a long, complex computer related crime case. Available funds for outside technical assistance will have some impact, though not necessarily definitive impact, on whether and where to turn to outside experts for help.

3.4.5 Availability of Local Resources

As a general rule, the greater the availability of local resources for outside technical assistance, the greater th temptation to call in outside experts early in the case, and throughout. As has been noted, many sources of expertise can be tapped at little or no cost, so the bringing in of outside expert may not be governed principally, if at all, by cost. Sections 4.0 and 7.0 suggest several case management considerations that, independent of cost, would argue for limiting the numbers and degree of involvement of outside experts to only that which is truly vital to breaking the case and/or obtaining the conviction

4.0 SELECTING AN EXPERT

The first step in the process of selecting an expert consultant/witness is the identification of one's specific technical assistance requirements. Once these needs have been defined, the selection of an expert can commence. There are computer operators, scientists, electronic engineers, systems analysts, media librarians, security specialists, data base managers and EDP auditors, to name a few of the job functions and areas of specialization. One must know enough about computers to begin with to know the area(s) in which assistance is needed. Lacking that knowledge, one must not be afraid to ask questions or engage in some quick self-education on computers. There are many good books and manuals available and also many good computer orientation courses now accessible through universities and vocational schools or other training facilities. If quick, informal preliminary advice is needed as to whom to confer with regarding computer systems, a trusted independent auditor, systems analyst or security administrator may be the single best initial entry point to the world of computers--which incidentally, is not quite as alien as it may at first appear.

The process of consultant identification and selection involves several factors which will inevitably bear directly on the outcome of the investigative or prosecutive effort. These important considerations will be discussed in this Chapter. They include financial considerations; the question of what requisite expertise a technical adviser in a given subject area must possess; the general criteria and standards for evaluating an expert's qualifications; the personal qualities which an otherwise qualified expert must display in order to be effective in his role; the importance of distinguishing the expert's true area of competence from other areas of his interest; a review of which types and categories of specialists are most likely to be needed at each key phase of a computer related crime case; and a general review of the sources of expert referral.

4.1 Financial Considerations

As indicated in Chapter 3.0, obtaining the services of experts in the investigation of major crimes such as computer frauds need not entail a great expenditure for the investigating or prosecuting agency. Experts can often be "borrowed" without cost from other law enforcement agencies or from other departments of State or local Government in one's jurisdiction. Employees of the victimized business or organization are often among the best technical advisers in such cases, and are frequently loaned by the victim as a public service as well as out of financial self-interest. Professional associations and other groups in the victim's industry may also be good sources of no-cost technical assistance, as may local area universities. While there are various disadvantages which can accrue from the use of some of these types of gratis experts, as noted in Section 2.2, above, generally the availability of such services without cost should be thoroughly explored as the first step in selecting an expert for a particular task.

Circumstances can, however, dictate that paid experts are advisable, or necessary, in certain areas of the case. What follows addresses important factors to keep in mind when considering a paid consultant or expert witness.

4.1.1 Availability of Funds

The amount of money which the agency and the particular unit responsible for investigating and/or prosecuting a computer related crime case has for such activities is obviously a threshold question. Absence of funds may substantially simplify the selection of technical advisers or even dictate that the investigation must proceed through use of only in-house resources. In such circumstances, however, local law enforcement and prosecutorial agencies would be well-advised to consider pooling resources with counterpart agencies at the State or Federal level, or with law enforcement in other jurisdictions, where a complex case is involved that appears to span jurisdictional lines.

Assuming that a significant amount of money might have to be invested in outside technical assistance by the local law enforcement agency initiating a computer related crime investigation the National District Attorney's Association recommends proactively budgeting for consultants before their assistance is actually needed in a given case. In its recent publication entitled Prosecutor's Manual on Economic Crime, NDAA suggests that,

> the prosecutor's overall budget should contain adequate funding to enable the economic crime unit to retain the services of expert consultants for actual investigations, for trial preparation and, where required for trial assistance and expert testimony.
>
> ....
>
> Extensive expert consulting services will be on a fee for service basis at the going consulting rate for the professional discipline involved. Operating experience on a jurisdiction-by-jurisdiction basis will determine the general annual consulting fee requirements for the economic crime unit. A

> regular budgeted consulting line item for the economic crime unit should be included in the unit's overall budget. (Emphasis original.)1/

The same recommendation is applicable to investigative agencies.

The NDAA Manual goes on to recommend that for an economic crime unit in a major jurisdiction, one trial attorney per 100,000 residents should be budgeted, with two investigators per trial attorney and two clerical support staff for each four professionals in the unit.2/ For a jurisdiction with 700,000 to one million residents, the NDAA Manual recommends 100 person days of consultant time at $100/day be budgeted along with full-time staffing costs.3/

Whether local law enforcement agencies investigating white collar crime, financial crime and computer crime can obtain budgetarily the level of consultant time recommended by NDAA is problematic. Local fiscal situations, political considerations, public attitudes toward economic crime, internal department procedures, etc. will all impact on the practicality of achieving or even exceeding this level of budget support.

4.1.2 Reasonable Compensation Levels

Presuming a law enforcement agency can afford to pay for technical assistance in a computer related crime case and that the services of a paid expert are required, the question arises, what is a reasonable level of compensation? This question, while critical, is extremely difficult to answer, for the following reasons:

- The types of experts who might be used at various stages of the case can come from a wide range of professional backgrounds. Salary structures and billing practices can vary tremendously among the relevant industries and professions,e.g. forensic chemists versus EDP programmers knowledgeable in COBOL.

- For two experts in the same speciality area--for example, computer security--billing rates will vary significantly based on the extent of prior experience and the complexity of the industry or business which has been the victim of the computer crime and with which the expert is expected to be familiar (e.g. banking versus retailing).

- The general availability of knowlegeable experts in a given speciality will also have a direct bearing on their cost; some types of specialists will be readily available locally while others will prove hard to find, may require financial incentives to induce them to travel, and will have travel costs. A closely related consideration is the following: The comparative abundance of qualified candidates will make itself felt to some degree in a competitiveness in their fee structures, while comparative exclusiveness of other sorts of expertise will allow those who are qualified to more successfully dictate their own price.

- Especially in the EDP technology fields, because their advent is so recent, generally-accepted billing rates for serving as consultants to Government have not yet been established. This puts both the law enforcement agency seeking outside services and potential service providers at a disadvantage.

- As with other types of professional services, e.g. legal services, real estate brokering, etc., fee structures vary significantly as between urban, suburban and rural areas, from one locale to another, from State to State, and regionally. The services of a qualified external EDP auditor who has served previously as an expert witness for example, could be expected to differ greatly in cost from one jurisdiction to the next, depending on the "going rate" locally.

In light of the above factors, it is impossible to accurately predict the cost of various sorts of outside expert assistance in an across-the-board fashion.

In an effort to provide some guidance and direction in this difficult and complex area, it is strongly recommended that the following facts be taken into consideration whenever planning, budgeting or negotiating for outside expert services in a computer related crime case:

- Federal regulations relied upon to determine reasonable levels of daily compensation for expert consultants whose services are procured by the U.S. Department of Justice provide several good standards that local law enforcement agencies could adopt: DOJ regulations base an expert consultant's daily fee on one of the following: (1) the equivalent of his or her daily income from the relevant activity in the outside work world (i.e. dividing the salary by 260 workdays); or (2) where the consultant is a corporation or self-employed, the equivalent of the daily billing rate, where there exists a reviewable billing history for such services; or, where neither of the above two approaches is appropriate, (3) the equivalent of what is the average daily fee in the given profession, field, or speciality area. Under such a tripartite approach the daily rate for Government work "floats" but is tied to demonstrable income or billing structures in the private sector.4/

- Many professions have very different billing rates for Government work versus private clients. For example, lawyers and psychologists will often command very high daily rates in the private sector but will employ a different fee structure--and therefore lower daily rates--for Government consulting. This is especially true where the Govenment agency is seeking their review of the work of others or their advice on how to proceed rather than commissioning them to perform the demanding professional activities for which they are retained by private sector clients, i.e., trying a case or performing psychoanalysis. Such experts should be asked about differential billing rates for Government service; where they have not previously consulted for Government, a differential rate should be suggested.

- Many independent consultants charge a daily rate which encompasses only a base fee for their personel professional services. Others who are self-employed, or who are employees of profit-making companies include in their daily rate, in addition to the base fee, an amount which covers a portion of their cost of doing business (overhead burden, general and administrative burden), i.e. fringe benefits, rental and maintenance costs for their physical plant etc. and other indirect costs. Some professional consultants will also request a fixed fee in addition to the direct labor (i.e. salary equivalent) and indirect cost burdens. Indirect costs and/or fixed fees can greatly increase the total daily billing rate for some private consultants, and consequently greatly increase the cost of such services to local law enforcement. Such added costs are generally legitimate and necessary expenses which are reasonably passed on to the customer. However, other consultants do not pass on such costs, due to a variety of factors, which are generally tied to the fact that they work in organizations which have alternative methods of defraying costs, i.e. universities, foundation-supported or government-supported research centers, etc. The presence or absence of indirect cost factors in a requested fee can have important budgetary implications.

- A number of professional associations, Government regulatory agencies and public service groups exist which will provide information upon request about prevailing billing rates for various types of consultant services. Such organizations should be contacted at the major case planning and budgeting stages, as well as later on to assess the reasonableness of a rate requested by a given outside consultant.

- Compensating an outside consultant on a day-to-day basis for the number of days worked is not the only way to proceed. Moreover, this approach may not facilitate advance budgeting nor insure the husbanding of scarce financial resources. Instead, it may be desirable for law enforcement agencies to consider contracting with outside experts on a fixed fee basis--so much money in return for the performance over time of certain clealy specified tasks, payment to be made in full at the satisfactory completion of the work, or pro-rated at certain intervals.

As indicated above, both the range of possible types of experts needed and the complexity of factors that would determine a daily rate for each type is so great that no general figures, in dollars, can be presented as a yardstick against which to measure likely costs or the reasonableness of fees requested. However, Exhibit A presents a suggested checklist of data to be gathered and factors to be taken into consideration when anticipating overall consultant expenditures in advance of commencing a computer related crime case.

4.1.3 Balancing the Competing Interests

Obviously, there are no easily generalizable answers to the questions, when should paid consultants be used? and, what amount of compensation is reasonable versus excessive? The facts and circumstances not only of every case, but of every local fiscal, political and administrative situation will differ, thereby dictating different answers to these questions from one agency to the next, and, over time, for the same agency. However, several overall trade-offs will be present in every case and must always be made. These include the following:

- What is the comparative importance of breaking this case/obtaining convictions against these defendants versus the same considerations for other ongoing cases in the unit or agency, in terms of overall budget allocations?

EXHIBIT A

SUGGESTED CHECKLIST FOR DETERMINING TECHNICAL ASSISTANCE NEEDS IN COMPUTER RELATED CRIME CASES

CATEGORY OF EXPERT	NEEDED IN THIS CASE? YES OR NO	IDENTITY OF EXPERT	SOURCE OF REFERRAL	FEE CHARGED? YES OR NO	AVERAGE FEE IN EXPERT'S FIELD ($/DAY)	SOURCE OF AVERAGE FEE DATA	DAILY FEE NEGO-TIATED
Computer Scientist							
Electronics Engineer							
Telecommunications Engineers							
Computer Crime Scholar							
Subject Area Expert							
EDP Programmer							
Systems Analyst							
Data Base Manager							
EDP Auditor							
Computer Security Specialist							
Computer Equipment Manufacturer/ Vendor							
Computer Services Rep.							
Forensic Chemist							
Document Examiner							
Other							
Other							

- What is a reasonable cost outlay for this computer related crime case when assessed against the comparative importance of the case?

- How can available financial resources best be conserved and applied in light of the anticipated length of the investigation and complexity of the case?

- In what aspects/areas of the investigation will the services of paid experts be essential versus nice-to-have, and what are the ranked priorities when matched against available consultant dollars?

- When should a less expensive/less-well-qualified expert be used rather than a more expensive/best-qualified expert, and vice-versa?

4.2 Requisite Qualifications Will Vary With The Expert's Speciality Area

Apart from the question of whether paid or unpaid experts are utilized and whether, if unpaid, their services are loaned by Government, industry or other sources, what are the requisite qualifications such experts must possess? What standards should be employed against which to assess the adequacy of a given specialist's credentials, and what criteria should be applied to select one possible expert over another?

As noted in Section 2.3, the range of fields from which possible technical advisers in computer crime cases can be drawn is substantial. Most of these are areas of technological specialization, though others are made up of persons with backgrounds in law, the physical sciences, the social sciences, business and finance. Requisite qualifications to serve as an expert, therefore, will vary from field to field.

As a general rule, formal qualifications--credentials--become critically important once the decision is made to put an investigative or pretrial technical adviser on the stand, thereby rendering him or her a potential expert witness, whose identity and qualifications become discoverable.[5] The practical, "hands-on" experience in a given subject area is the paramount qualification of a behind-the-scenes expert during the early phases of the case. However, the possibility--under some circumstances, likelihood--that the adviser will have to "go public" and take the stand argues strongly for the selection of experts at all stages who display the demonstrable formal qualifications, and personal characteristics, necessary to insure their acceptance by the court as experts in their respective fields and to sustain their credibility as experts in the face of cross examination and defense efforts at impeachment. Even if the behind-the-scenes expert is not designated as a potential expert witness, his identity and qualifications, or the nature of the expert's relationship with the Government or the victim may become discoverable.6/

Table 7 presents a matrix of relevant credentials and key types of computer related crime experts. Check marks (X) indicate those formal qualifications likely to be of importance for each category of expert, both in terms of their practical value behind-the-scenes and, more directly, their acceptability as credible expert witnesses at trial. The importance of each set of credentials is discussed in detail in Section 4.3.1, below.

TABLE 7
OCCUPATIONAL CATEGORIES OF COMPUTER CRIME EXPERTS AND COMPARATIVE IMPORTANCE OF KEY CREDENTIALS

	PRIMARY CATEGORIES OF CREDENTIALS							
CATEGORIES OF COMPUTER RELATED CRIME EXPERTS BY OCCUPATION	LICENSE OR CERTIFICATION	ACADEMIC DEGREE(S)	TRAINING AND CONTINUING EDUCATION	WRITINGS AND PUBLICATIONS	TEACHING, LECTURING AND CONSULTANCIES	PROFESSIONAL ASSOCIATIONS	PRIOR DIRECT EXPERIENCE	ACCESS TO PRIVILEGED INFORMATION
COMPUTER SCIENTISTS	X	X	X	X	X	X		
ELECTRONICS ENGINEERS	X	X	X			X	X	
TELECOMMUNICATIONS ENGINEERS	X	X	X			X	X	
COMPUTER CRIME SCHOLARS, RESEARCHERS AND/OR LEGAL COMMENTATORS	X	X	X	X	X	X	X	
SUBJECT AREA EXPERTS FROM VICTIM INDUSTRY	X	X	X		X	X	X	
COMPUTER USERS IN VICTIM'S EMPLOY			X				X	X
DATA PROVIDERS IN VICTIM'S EMPLOY			X				X	X
COMPUTER OPERATORS IN VICTIM'S EMPLOY			X				X	X
EDP PROGRAMMERS (INTERNAL AND EXTERNAL)			X		X		X	X
SYSTEMS ANALYSTS (INTERNAL AND EXTERNAL)			X		X	X	X	X
DATABASE MANAGERS (INTERNAL AND EXTERNAL)	X		X		X	X	X	X
EDP AUDITORS (INTERNAL AND EXTERNAL)	X	X	X		X	X	X	
COMPUTER SECURITY SPECIALISTS (INTERNAL AND EXTERNAL)	X		X		X	X	X	X
HW/SW MANUFACTURERS/VENDORS			X				X	X
COMPUTER SERVICE INTERFACING WITH VICTIM			X				X	X
EXPERIENCED CRC INVESTIGATORS	X		X		X	X	X	
FORENSIC SCIENTISTS	X	X	X	X	X	X	X	

4.3 General Criteria and Standards for Evaluating An Expert's Qualifications

A determination that a given person is sufficiently knowledgeable and capable to serve as an expert in a computer related crime case will depend on two broad factors. First, does the candidate possess the objective qualifications for the job? Does he or she possess the appropriate credentials, have relevant prior experience, and/or be in possession of critical information having a bearing on successful resolution of the case?

Second, does the expert, albeit sufficiently qualified, display the personal characteristics that allow him or her to effectively function as part of the investigative team? Is the individual a team player? Does his or her professional reputation and the quality of previous work recommend usage in the case at hand? Can the expert explain technical complexities in such a way that criminal justice practitioners--investigators, prosecutors, judges--as well as laymen--the jury--can clearly understand their meaning and importance? Does the expert project a professional manner? Can he or she build and keep rapport with others? The following subsections address in detail both the requisite formal credentials and the essential personal charactertistics which effective consultants and expert witnesses must display.

4.3.1 Credentials

Credentials and standards for assessing the knowledgeability of out-of-court experts will vary, as noted above, depending on the area of expertise. Even with regard to laying the foundation at trial for a witness' acceptance by the court as an expert, the criteria, though generally standardized between fields of expertise in the eyes of the law, are not inflexible and are subject to some variation. With these caveats in mind, there are several broad areas in which experts are expected to display credentials and qualifications which distinguish them from the laymen. These include the following:

- professional licensure, certification, or registration by a recognized professional body in the field of expertise in question;
- relevant undergraduate, graduate, and post-graduate academic degrees directly in the field of expertise or a suitable background to it;
- specialized training and/or continuing professional education beyond academic degrees that indicates up-to-date familiarity with the latest technical developments in the expert's subject area;

- the expert's writings and publications that display technical opinions and which are available as part of the general body of knowledge in the subject area;
- relevant teaching, lecturing and/or other consultancies undertaken by the expert, which indicate that he or she is held in high professional esteem in the given subject area;
- professional associations with which the expert is affiliated;
- directly relevant prior experience which the expert has gained through undertaking similar assignments, whether as technical adviser or expert witness, in the given subject area; and
- special status, or access to privileged information, peculiar to the case at hand which renders the individual an expert because he is in possession of unique facts.

The following subsections address the comparative importance of each of these credentials in further detail. How they impact on the effective utilization of the expert in the case is addressed in Section 6.0 of this Manual.

4.3.1.1 Professional licensure, certification or registration

Most professionals to some degree regulate their members and feature mechanisms for reviewing a practitioner's qualifications--often at periodic intervals. Endorsements as to competence--a license to practice the profession, a certification of compliance with training or continuing education requirements in a speciality area, or registration at a central authority in the jurisdiction for purposes of regulating the profession--are all common practices. As Table 7 illustrates, the presence of a professional license, certification or registration is an important factor in assessing the level of basic competence for technical advisers in most areas of expertise useful in computer related crime investigations (with the general exception of persons in the victim's employ, or who interfaced with the victim's operations, and are experts because they are in possession of unique facts). Establishing that an individual possesses a license or certification in his or her profession, and/or is registered in the jurisdiction as a practitioner of that profession, is a standard step in laying the foundation at trial for the court to accept the testimony of such an individual as expert.

Determining what standards are used to qualify a practitioner in a given profession can easily be determined by inquiring of the professional licensing or certifying body in question. In addition, many jurisdictions require practitioners of a wide variety of professions, and who may have acquired their credentials elsewhere, to register with a central Government authority if they desire to practice their profession locally. Table 8 presents and identifies the central professional registering authorities for most States. The central registering authority can be a useful source of information on professional licensing standards locally and perhaps a source of expert referrals. In addition, this office or agency will be in a key position to confirm the bona fides of a particular expert the Government is considering retaining or that of a defense expert whose identity in advance of litigation has been discovered.

As we have seen, many of the more traditional professions supply experts to computer related crime cases. Thse include lawyers, engineers, forensic chemists, etc. Most States have laws on the books which dictate the criteria for professional licensing in these broader professions. However, qualifications for many of the new computer technology fields have not yet been a subject of State Government regulation, nor has the private security industry from which many physical security and data base security consultants who are potential computer related crime experts are drawn. By way of example of the current differences between States on the regulation of such "new" computer related professions, Table 9 illustrates which States at present have laws on the books to regulate the licensing of private security consultants.

4.3.1.2 Academic degrees

The presence of appropriate academic degrees has traditionally been a key indicator of whether an individual will qualify as an expert witness.[7] Even where an expert is being utilized in a computer related crime case as a behind-the-scenes technical adviser at the investigative or pretrial stage, the fact he or she may be a "potential expert witness," or that the nature of their employment retention, qua consultant, is discoverable by the defense, the presence or absence of academic credentials will be a relevant consideration when assessing overall utility and credibility of an expert.[8]

Generally speaking, the requisite academic degrees for each profession and the identities of those institutions of higher learning whose degree programs are accredited are key facets of State or local licensure, certification or registration laws or regulations, as discussed in Section 4.3.1.1, above. State or local laws should be consulted on this point.

Table 8

State Regulatory Agencies Which License And/Or Regulate Many Types of Technical Experts

State	Regulatory Agency
Arizona	Department of Public Safety
Arkansas	Department of Public Safety
California	Department of Consumer Affairs
Colorado	Department of State; Office of the Attorney General
Connecticut	State Police
District of Columbia	Metropolitan Police Department; Department Licenses and Inspections
Florida	Department of State
Illinois	Department of Registration and Education
Indiana	Superintendent of State Police
Iowa	Commissioner of Public Safety
Kansas	Office of the Attorney General
Kentucky	County and Municipal Clerk
Maine	Commissioner of Public Safety
Maryland	Superintendent of State Police
Massachusetts	Department of Public Safety
Michigan	State Police
Montana	Department of Professional and Occupational Licensing
Nebraska	Secretary of State
New Hampshire	Department of Safety
New Jersey	State Police
New Mexico	Office of the Attorney General
New York	Department of State
North Dakota	Office of the Attorney General
Ohio	Department of Commerce
Oklahoma	Local Chiefs of Police
Oregon	Private Securities Industries Board
Pennsylvania	Local Police Departments
South Carolina	Chief, State Law Enforcement Division
Virginia	Department of Professional and Occupational Regulations
West Virginia	The Secretary of State
Wisconsin	Department of Regulations and Licensing

Table 9

States Which License and Regulate Private Security Consultants

STATE	LICENSING REQUIREMENTS?	STATE	LICENSING REQUIREMENTS?
Alabama	No	Nebraska	Not Listed
Alaska	Yes	Nevada	Yes
Arizona	Yes	New Hampshire	Yes
Arkansas	Yes	New Jersey	Yes
California	Yes	New Mexico	Yes
Colorado	Yes	New York	Yes
Connecticut	Yes	North Carolina	Yes
Delaware	Yes	North Dakota	Yes
Florida	Yes	Ohio	Yes
Georgia	Yes	Oklahoma	No*
Hawaii	Not Listed	Oregon	Yes
Idaho	No*	Pennsylvania	Yes
Illinois	Yes	Rhode Island	No*
Indiana	Yes	South Carolina	Yes
Iowa	Yes	South Dakota	No*
Kansas	Yes	Tennessee	No*
Kentucky	Yes	Texas	Yes
Maine	Yes	Utah	No*
Maryland	Yes	Vermont	No*
Massachusetts	Yes	Virginia	Yes
Michigan	Yes	West Virginia	Yes
Minnesota	Yes	Wisconsin	Yes
Mississippi	No*	Wyoming	No*
Missouri	No*	District of Columbia	Yes
Montana	Yes		

* Check City and/or County Ordinances

Despite the strategic importance of appropriate academic credentials for experts whose credibility may be challenged by the defense, with regard to the more technological aspects of the problem, over-reliance on academic credentials for experts in computer related crime cases must be cautioned against. Many universities do not have well developed courses, especially post-graduate, in this area. In addition, technological advances are occurring so rapidly that many educational programs are not current. Knowledgeable sources agree fairly consistently that an expert's academic preparation for his discipline should certainly be weighed and considered very carefully but of equal importance can be how recently the degree was taken and what other continuing education courses have been taken along the way.

4.3.1.3 Training and continuing education experience

As noted in Section 4.3.1.2, technological developments in computer programming, electronics and telecommunications engineering, EDP auditing, computer security and other specializations are occurring increasingly rapidly. Courses of training and continuing education in these areas, as in topical areas such as combatting white collar crime, economic crime and computer crime, are being widely offered. Certificates of completion and other objective indicators of ungraded skills as a result of attendance at such courses are frequently offered by professional associations and regulatory bodies.

How many current, relevant training courses and continuing education courses have been attended by the prospective technical expert? How up-to-date is he or she on the state-of-the-art in this technical field? A showing of such currency is generally a corollary to the presentation of academic credentials to the court at the time an expert witness' qualifications are reviewed.[9] The absence of such current educational updates can be expected not only to impact on the quality of expert advice given to the Government but can lead to impeachment of the Government's expert witness on cross examination and to the challenging of the technical accuracy of aspects of the Government's case when the identities and qualifications of behind-the-scenes technical advisers relied on when preparing the case are discoverable.[10]

4.3.1.4 Writings and publications

Whether a prospective expert witness has published in the field of his or her purported expertise is traditionally an important factor to be reviewed when laying the foundation at trial for the technical adviser to take the stand as an expert witness.[11] Prior publications may be of less relevance when the expert is used as a technical adviser to the investigative or prosecutive team during the case preparation stages. However, this is not necessarily the case. The prior publications of a computer related crime scholar/researcher who has been retained to assist in profiling the computer felon(s) and determining modus operandi in a complex computer fraud case will be of direct relevance. Their availability could greatly assist the team by way of orientation, and such published views could be challenged if the technical adviser's identity is discoverable pretrial.12/

What books or articles has the technical adviser written on the subject in question? Were they published and, if so, how recently? How were the expert's works received by his or her professional peers? Are the expert's works considered authoritative? Do other published works in the same field challenge or contradict the expert's published views? Are the expert's published views consistent in all of his or her writings? Are his or her published views, while consistent among themselves, congruent with the expert's current views espoused in the case at hand? These are all critical questions to be addressed when selecting an expert. Especially if there is to be an established or prolonged professional relationship with the expert, the initiative must be taken to analyze the consultant's published works and to later monitor the pretrial preparation process to avoid any significant discrepancies which may arise between present, planned testimony by the expert and past, possibly contradictory, positions he or she has taken.

4.3.1.5 Teaching and other consultancies

Activities which evidence a consultant's prior acceptance as an expert adviser or instructor go to the issue of his or her reliability and credibility as part of the Government's team. Such activities as teaching or consulting in a given field are traditionally considered at the time an expert's credentials are presented to the court in preparation for taking the stand as an expert witness.13/ Because of the newness and rapid evolution of computer related technology, such credentials may hold more weight in a computer related crime case than academic degrees or publications. A careful reference check with past consumers of the prospective expert's services--trainees or clients for whom he or she has consulted--can be an excellent way to assess that expert's reliability and stature, plus the currency and nature of his or her views, in advance of retention in a given case.

Extensive prior teaching and/or consultancies on the part of the Government's expert can, if he or she has been retained for a fee, sometimes work to the detriment of the prosecution. For example, an expert who for a fee has done extensive training of investigators and prosecutors in the area of computer crime, and/or who has for a fee testified frequently for the prosecution in such cases, but not for the defense, could be impeached for bias and/or financial interest if called as an expert witness by the Government.[14] Especially where a substantial percentage of an expert's income derives from such services to law enforcement, his or her comparative utility as an expert witness may be comprised.[15]

Even if such an expert is not a potential expert witness, his identity and involvement in the preparatory stages of the case may prove discoverable by the defense and lead to allegations of bias in the technical advice rendered at the investigatory stage.[16] These considerations aside, retention of an expert who has extensively trained and consulted for only one side in such cases can greatly lessen the fundamental value of having an outside expert on the investigative team to begin with--his or her objectivity when dealing with complex technical issues.

4.3.1.6 Professional associations

As in the case with professional licensure, certification or registration, membership by a prospective expert in professional associations representing practitioners in the given subject is a credential which gives added weight to a presumption of competence and which is routinely included in the proffer of an expert's credentials to the court preparatory to the presentation of expert testimony.[17] As with the matters of licensure, academic degrees, continuing education, and prior consultancies, membership in professional associations is subject to verification checks and to the gathering of references from the expert's professional peers. This is an important and useful quality control check which should always be taken advantage of, regardless of whether the technical adviser is viewed as a potential expert witness.

4.3.1.7 Previous similar experience

As noted in Sections 1.2 and 2.3, due to the newness of the various computer technology fields and the speed with which new developments in computer technology are taking place, formal credentials are often of less importance in computer related crime cases than is direct prior experience with the victim company's computer operations, the brands of hardware or software used by the victim, the programming language involved, etc. In addition, prior experience at investigating computer related crimes, at providing computer security, or at computer related crime research can be the critical element that renders a particular party an expert adviser. Identifying trustworthy and objective advisers who possess such direct prior experience can, as has been noted elsewhere in this Manual, be the single most important aspect of selecting an expert. Despite the existence of traditional criteria, such as formal credentials, by which a proffered expert's qualifications to testify as an expert witness are normally assessed, the trial judge has broad discretion to base a decision that an individual is an expert qualified to testify on a given subject primarily--or even solely--on that person's prior relevant experience.18/

As noted in Section 1.2, above, and in Section 7.0, there are pitfalls in over-reliance on technical advisers with extensive prior experience in the subject area. Maintaining control over the overall management and direction of the case can be one difficulty. Susceptability to defense charges of partisanship and bias against experts with extensive prior experience which is disproportionately on the Government's side only of such cases is another hazard. Regardless, this remains the single most important qualification to provide technical assistance in the ever-changing arena of computer related crime.

4.3.1.8 Access to privileged information or unique facts

As noted in Section 2.2, employees of the victimized agency or of the manufacturer, vendor or service organization whose computer products the victim utilized can be among the most useful of technical advisers when investigating a computer related crime case or preparing one for trial. The backgrounds, education levels, and other credentials displayed by such persons can be expected to vary tremendously; this group will span top management at the victim organization, its in-house computer technologists, its data providers, equipment operators and others who handle relevant data or are in possession of unique facts about the victim's operations. As a result, qualifications for such persons in their respective fields, while important, will prove secondary to their familiarity with aspects of the victim's operations and equipment. For the narrow purpose of laying out what such operational practices routinely were or what equipment capabilities and vulnerabilities are, courts can be expected to admit expert testimony from such persons, provided the prosecution is able to demonstrate the expert witness' close familiarity with such factors and his or her general competence.

The greatest pitfalls in the use of such individuals as pretrial technical advisers or as expert witnesses at trial, obviously, are (1) distinguishing the true area of competence and (2) bias. Employees or service personnel may be qualified to speak authoritatively on only very narrow points and be completely unqualified on other, related points. In addition, loyalty to the employer, job security considerations or, on the other hand, a grudge against the employer or another employee may taint the individual's objectivity and hence utility. And, of course, the investigative team must be especially circumspect about bringing such persons in as technical advisers unless and until their possible complicity in the crime has been completely ruled out.

4.3.2 Personal Qualities of the Expert

Apart from credentials, the other primary set of standards against which must be measured the advisability of utilizing a given individual as a technical adviser or expert witness consists of the qualities of the prospective expert. Because this area is primarily subjective, as distinguished from the relative objectiveness of credentials, a presentation of what constitutes the key factors and how they should be assessed is difficult. However, eight generic considerations have been isolated which hold true for the use of technical advisers or expert witnesses in any major case, whether or not computer related. The following subsections present these considerations.

4.3.2.1 Ability to work as part of a team

Many individuals, regardless of the area of their professional competence, are not temperamentally or attitudinally geared to working as part of a team. Doubtless, this problem is more prevalent with certain professions than with others due to the nature of the work performed and other factors. Assessing whether a prospective expert will be a team player is a critical decision that must be made at the earliest stage of the relationship--before the expert is retained. Reference checks and personal interviews are tools in making this determination. Effective management of the expert in the case, the security of sensitive investigative data, and the effectiveness of the expert as a witness on the stand are only a few of the overriding considerations that dictate utilizing only "team players" in expert roles.

4.3.2.2 Trustworthiness and integrity

Despite the advisability of limiting a technical adviser's access to casework on a "need-to-know" basis, the expert will invariably be exposed to sensitive information during the course of the case. At very least, this will extend to a knowledge of his own role in the case, conversance with those aspects of the investigation where he or she has been providing input, and the identities of others on the investigative team. The trustworthiness and discretion of the expert must be assured and maintained. Section 5.0 presents a variety of techniques which are useful to employ to maintain the investigative integrity of the case. However, in the final analysis, the expert's integrity and discretion must be relied on to avoid breaches of security.

As with the problem of insuring that the expert is a team player, detailed reference checks and personal interviews must be utilized to make a preliminary determination as to the expert's trustworthiness and integrity.

4.3.2.3 Professional reputation and recognition

A concomitant qualification to academic degrees and publications will be the notariety of the expert and the professional reputation which he or she enjoys among their peers. While this will in part be a product of the authoritativeness of the expert's views and the prestigiousness of his or her formal credentials and experience in the field, it will also be reflective of the personal qualities which the expert displays. Many of these qualities will be directly relevant to whether the expert will be a good candidate for a harmonious working relationship with others on the case.

The expert's notariety can cut both ways with regard to his or her credibility as an expert witness on the stand: If his or her views are controversial or even contested, the greater the expert's notariety, the more likely the defense will be able to identify counter-experts familiar with the views and at odds with them. On the other hand, increased notariety can go to the issue of stature and authoritativenss, by which opposing expert opinion can be overshadowed.

Reference checks and a review of the literature in the field to accurately gauge an expert's professional stature and notariety are important steps to be undertaken in advance of retention. Even if the expert is not to be retained as a potential expert witness, the nature of his or her role in the case or the nature of the retainer agreement can make the expert's identity discoverable by the defense at the pretrial stage and, thus, open to attack his or her professional reputation and stature in the field.19/

4.3.2.4 Quality and timeliness of previous work

It will be of critical importance to assess, in advance of retaining an expert, the quality of his previous work. Most directly, the quality of his or her prior consultancies and service as an expert witness must be checked out in great detail. In addition, the general perception in the professional community as to the quality of the expert's work--publications, teaching, lectures, etc.--should be determined. If the Government's expert is a potential expert witness, it can be assumed that the defense will make a thorough assessment in this area, and will attempt to impeach. The investigative and prosecutive team cannot afford surprises on cross examination in this regard. Employers, prior clients, professional references, and professional and regulatory agencies, among others, should be contacted for an assessment of the quality and timeliness of the prospective expert's work.

4.3.2.5 Professional bearing and demeanor

Of perhaps subtle but always significant importance is the professional bearing and demeanor of the technical adviser. For potential expert witnesses, the ability to speak authoritatively, to sustain composure under vigorous cross-examination, to avoid argumentativeness with opposing counsel and to simplify for the judge and jury without condescension are essential characteristics to be displayed, the absence of any of which should screen the admitted expert out of the consideration as an expert witness. However, these and other qualities must be present in the behind-the-scenes technical adviser, too, who must work closely with the other members of the investigative team, often under pressure.

Determining professional bearing and demeanor can be complicated. Initial impressions during interviews and preliminary discussions about the case are important, as are assessments by references and other outsiders. However, all of these observations are of limited utility. Engaging in role play early in the process--with other investigators or prosecutors simulating an interrogation or cross-examination--will display useful information about the expert's reactions under pressure and in response to challenges to his expertise. Playing devil's advocate in a discussion with the expert about his views or opinions on technical issues, or asking the expert to discuss the weaknesses in his own positions, or probing the expert on subjects beyond the area of expertise to assess the degree to which he or she is opinionated by nature are also useful techniques. In short, stress interviews for experts, whether or not they are viewed as potential expert witnesses, are an essential tool to gauge bearing and demeanor.

4.3.2.6 "Presence" before a group

The ability to effectively present ideas to a group is a learned skill; however, many individuals in all areas of endeavor lack this skill. An expert whose knowledge of a technical area is sound and who can effectively advise investigators behind-the-scenes may or may not possess an effective "presence" before a group.

This will be a critical skill in any expert witness; for potential expert witnesses, advance screening for the presence of this skill and practice sessions to enhance it for trial are a must. However, the ability to make effective presentations to groups may also be a necessary attribute of the behind-the-scenes technical adviser; this factor should therefore be taken into consideration when retaining any expert.

Advisers at the investigative or pretrial stages of complex cases may be called upon to give orientation sessions on technical aspects of the case to a large group of investigators and other technical advisers. This will require the expert to be effective at group presentation. In addition, should the identity of the technical adviser become known to the defense at the pretrial stage, depending on the nature of his relationship with the Government and his role in the case, the expert may be subpoenaed to testify.[20] This would require him to have the same ability to effectively command the attention of a group as if he had been designated as a potential expert witness by the Government.

4.3.2.7 Articulation with laymen

A thorough grounding in one's field of expertise and the ability to make effective group presentations are undercut if a technical adviser is unable to simplify complex technical matters so that the intelligent layman can understand them. Indeed, this is the most fundamental skill which a techical adviser or expert witness must possess. The ability to make technical points understandable to the members of the investigative or prosecutive team will be critical to their ability to erect a sound theory of the case and to implement an effective strategy to break the case and/or obtain a conviction. Similarly, the ability to bring important technical points home to the judge and jury--without confusion or condescension--will directly impact on the likelihood of a favorable verdict.

If the expert has performed other consultancies in the past or served previously as an expert witness, determining whether he or she possesses this skill should prove easy by performing a thorough reference check. However, in the absence of these prior experiences, an effective technique would be to have the prospective expert explain to a group of lay office staff present in the office the meaning of a few technical terms or concepts selected by the interviewer. If the uninitiated observers cannot grasp the expert's explanation, chances are that other laymen on the investigative team and on the jury will not readily understand, either. The presence or absence of strong interpersonal communications skills in an expert is universally acknowledged as a key factor in the advisability of retaining him or her.

4.3.2.8 Mannerisms and idiosyncracies

Distractions distract. Idiosyncratic behavior such as peculiar mannerisms, unusual modes of dress, and other aspects of the expert's personality tend to deflect attention from the speaker's message to the speaker himself. Likewise, the use of vulgarity or excessive humor at inappropriate times in a presentation, or frequent ad hominen remarks about professional rivals would tend to alienate listeners against the speaker and thus against his message. Such distractions must be eliminated at all cost in the case of potential expert witnesses, either by behavior modification or replacement of the expert. Again, because behind-the-scenes technical advisers can under certain circumstances be subpoenaed to testify, these caveats are not limited to designated expert witnesses alone.

4.4 Sources for Identification of Individual Experts

As discussed in Section 2.2, technical advisers for use in computer related crime cases can be recommended by or drawn from a number of sources. These include the following:

- in-house sources,
- other law enforcement agencies,
- other agencies of State or local government,
- State and local licensing, certifying and registering bodies,
- law enforcement professional associations,
- professional associations in the subject area of expert knowledge sought,
- the victimized organization,
- the manufacturers/vendors and serving organizations who supply equipment or interface services to the victim,
- other organizations in the victim's field of activity or industry,
- area universities and research centers, and
- private consulting firms specializing in the subject area.

Determining which source(s) to go to for a particular sort of expert will be dictated by a mix of factors, including the following:

- prior experience at obtaining experts,
- available financial resources,
- pre-existing relationships with other agencies and referral sources, and
- the facts and circumstances of each case.

Table 10 presents a matrix of likely sources for technical advisers and expert witnesses in computer crime cases, arranged by type of expertise needed.

4.5 Distinguishing the True Area of Competence

A concluding consideration when selecting an expert is offered as a caveat: Be certain of precisely what area(s) of expertise the investigative team needs to tap other advisers for, and be careful to distinguish between these various areas of technical expertise when selecting a given consultant. For example, the decision to retain an EDP programmer, an EDP auditor and a computer security specialist as a core team of outside technical advisers when undertaking a complex computer related crime case will be a frequent decision. However, selecting a programmer who is proficient in the programming language of the victimized company will be equally essential. Likewise, selecting a programmer and an EDP auditor who are familiar with business applications of computer technology within the victim's field or industry will be a necessary distinction. Finally, when selecting a computer security consultant, the need for a physical security specialist, or a data security specialist, or both must be discerned. (Most computer security consultants are not expert at both aspects.) These examples could be expanded almost indefinitely.

Distinguishing the areas(s) of specialized expertise needed must be coupled with distinguishing the true areas(s) of a given consultant's expert competence from other areas in which he or she is not truly expert. This process is made more difficult because experts in one area are often unaware--or unwilling to admit--the limitations of their expertise. In situations such as these, reliance on representatives of the victimized organization or the manufacturers or vendors of the computer hardware or software equipment involved in the crime can be the best sources of guidance as to precisely what outside expertise is needed and what types of persons would be likely to possess the requisite capabilities. Consultation with experienced computer crime investigators or prosecutors, whether locally or from other jurisdictions, can be expected to be helpful on the more legal-related aspects of securing outside technical advice. Finally, the involvement of an experienced computer related crime

TABLE 10
LIKELY SOURCES OF TECHNICAL ADVISORS IN COMPUTER RELATED CRIME CASES BY TYPE OF EXPERTISE REQUIRED

TYPES OF EXPERTS REQUIRED	IN-HOUSE RESOURCES	OTHER AGENCIES OF GOVERNMENT	LICENSING BODIES	PROFESSIONAL ASSN'S IN SUBJECT AREA	LAW ENFORCEMENT PROFESSIONAL ASSN'S	VICTIM COMPANY OR ORGANIZATION	HW/SW MANUFACTURER VENDOR/SERVICERS	OTHER ORGANIZATIONS IN VICTIM'S INDUSTRY	AREA UNIVERSITIES, RESEARCH CENTERS	PRIVATE CONSULTING FIRMS	OTHER LAW ENFORCEMENT AGENCIES
COMPUTER SCIENTISTS		X	X	X		X	X	X	X	X	
ELECTRONIC ENGINEERS		X	X	X		X	X	X	X	X	
TELECOMMUNICATIONS ENGINEERS		X	X	X		X	X	X	X	X	
COMPUTER CRIME SCHOLARS			X	X	X				X	X	X
SUBJECT MATTER EXPERTS FROM VICTIM'S INDUSTRY				X		X	X	X			
COMPUTER USERS						X	X	X			
DATA PROVIDERS						X	X	X			
COMPUTER OPERATORS						X	X	X			
NON-COMPUTER PERSONNEL WHO INTERFACE IN VICTIM'S OPERATION						X	X	X			
EDP PROGRAMMERS	X	X	X	X	X	X	X	X	X	X	X
SYSTEMS ANALYSTS	X	X	X	X	X	X	X	X	X	X	X
DATABASE MANAGERS				X		X	X	X			
EDP AUDITORS	X	X	X	X	X	X	X	X	X	X	X
COMPUTER SECURITY SPECIALISTS	X	X	X	X	X	X	X	X	X	X	X
EXPERIENCED COMPUTER RELATED CRIME INVESTIGATORS	X	X	X	X	X		X		X		
FORENSIC SCIENTISTS	X	X	X	X	X		X		X		X

researcher or scholar could prove helpful when attempting to isolate the areas in which outside expertise will be required in the case.

5.0 PRIVACY AND SECURITY CONSIDERATIONS IN THE USE OF OUTSIDE EXPERTS

Sadly, the fact that an individual is an expert does not necessarily render him or her honest and trustworthy. While improper activities by experts are not likely, the potential for damaging actions by persons with access to sensitive information does exist, and should be addressed. Computer related crime cases like other white collar crime cases are likely to be fraught with complex technical issues that require the investigative/prosecutive team to turn to others for technical assistance at any or all stages of the case. Experts in such cases will be uniquely privy to sensitive data gathered during the investigation, to the internal workings of the Government's team, and to the details of the investigative and prosecutive theory of the case. As a result, the need for privacy and security safeguards on the use of outside experts in such cases is great. This section addresses these concerns.

5.1 Privacy and Security Considerations in Computer Related Crime Investigations

Computer related crime investigations and prosecutions may lead the team, including the consultant/expert, into some exceptionally sensitive areas. For this reason, special attention must be paid to security considerations. Some examples of these sensitive areas include access to national security matters, corporate trade secrets, legally privileged information, secret proceedings of ongoing investigative grand juries under a special deputization process, active criminal intelligence files and the proceedings from court-authorized electronic surveillance. Obviously, these possibilities represent some of the more extreme examples which would commensurately require a much higher level of security consciousness. Not all computer related crime cases will feature such aspects or raise such concerns. However, one or more of these special security areas tend to appear in major case investigations, especially in financial and other types of white collar crimes. Even where a computer related crime case does not at the outset appear to involve such aspects, it is important to appreciate that what may have begun as a routine investigation can quite conceivably and quickly turn into a very sensitive matter. In this respect, more long-range planning which seeks to anticipate these types of occurrences is essential. Good judgement and discretion are required as agencies proceed with complex cases in such new areas of law and criminal procedure.

5.2 The Necessity for Background Checks and Credibility Evaluations

In much the same way as novices tend to attribute to computer generated data absolute accuracy and infallibility, the uninitiated computer related crime investigator may be tempted to generalize from an expert's technical qualifications and assume that important personal qualities are present when this is not necessarily so. The fact that someone has specialized knowledge, advanced degrees and enjoys a professional reputation as an "expert" in a particular field does not necessarily mean he or she will be an asset or a good security risk in a sensitive computer related crime case. Many other factors must be considered in a background check and evaluation of the consultant from a security standpoint before this conclusion can be reached.

Several key factors must be considered when evaluating the prospective expert as a good security risk for inclusion in the investigative team. These include the following:

- any previous experience at classified work or sensitive cases, and demonstrable discretion;
- apparent financial stability and the presence or absence of any potential conflicts of interest relative to the case at hand;
- personal and professional ethics, as demonstrated through previous work and associations;
- amenability to guidance and direction, willingness to work as part of a team, and loyalty to group goals;
- respect for the right of privacy of individuals and organizations under investigation; and
- any previous history of unauthorized disclosure of confidential information.

How thoroughly a consultant is checked out will depend upon a variety of factors. Is he or she paid? What will be the extent of the expert's involvement? How sensitive is the case in which the expert's services will be utilized? Are the various aspects of the case compartmentalized or does everyone on the team know everything about the case? How closely and competently can the day-to-day activities of the consultant/expert be supervised by a known and trusted official member of the team? Has the expert in question been utilized by the agency before? If so, what was the previous experience and quality of the background check? What has the person been doing professionally since last contact? The answers to these and similar questions will dictate the nature and extent of the background check to be undertaken, as well as the limitations and safeguards placed on the consultant's utilization on the case.

5.3 Key Steps in Completing the Background Check

What should be required in conjunction with the background check? Again, this will depend somewhat on the specifics of each case. But in general, during the preliminary contact stage--negotiations and first interview--an authorization and waiver should be obtained for access to and examination of various records, including financial. In addition, a comprehensive and updated professional resume should be obtained which includes previous employers and references. The references should be checked carefully.

In addition, the investigators may decide to ask the prospective witness to suggest the names of professional rivals or competitors, or previous employers or clients with whom good relations have not been maintained and the reasons therefor. Any prominent person who has taken a stand on a disputed issue, engaged in legal related advocacy efforts, or published in an important field has developed rivals and antagonists. Persons are not always as reluctant to provide such information as one might assume at first. Reference checks with such persons should be undertaken, duly recognizing that the source will doubtless provide a negative reference. This approach is justified because it anticipates a defense strategy. If today's consultant becomes tommorrow's expert witness at trial, the investigative/prosecutive team will want to have some idea of whom the defense will bring in to discredit the expert, and have an idea of what they may say. If the consultant under review and consideration refuses to discuss his or her professional adversaries or detractors, then one must question that person's possible honesty and utility as a confidential technical adviser.

In any event, all positive and negative factors potentially affecting the credibility of a key witness who may later play the vital role of offering expert opinion testimony at trial must be fully explored and considered. As has been demonstrated on numerous previous occasions in computer related crime cases, the admissibility of evidence and subsequent outcome of a proceeding will very often hinge critically on the testimony of the expert. This should be considered during the credibility evaluation and background check.

Credit checks and a review of the expert's fiscal solvency are also key aspects of the background check. For example, experts or advisers who are employees of the victim organization, and themselves may have had the motive or opportunity to profit from the computer related crime are an obvious category of experts for whom large bank deposits or purchases, or a recent, sudden improvement in standard of living would be suspicious and must be investigated and explained. Technical specialists who are out of work or otherwise facing fiscal difficulties may be impeachable at trial by the defense as biased because they had a financial interest in the success of the litigation. Confidential "inside" advisers who are in possession of especially sensitive information in the case may be high risks for bribery if their financial situation is not good. These are only a few of the more obvious scenarios that suggest a thorough check of bank and credit references for prospective experts.

5.4 Special Security Precautions During the Course of The Investigation

For many major computer related crime cases, as for other types of white collar crime cases, a thorough background check alone will not provide an adequate assurance that the privacy and security of sensitive data will not be compromised by the outside consultant. Consequently, additional, special security precautions must be put in place and maintained throughout the course of the investigation. This section suggests several effective security precautions that could be employed.

5.4.1 Limiting Access to Sensitive Information to "Need-to-Know" Personnel

The larger and more complex a computer related crime case becomes, the more difficult a management challenge it presents. This situation will also lead naturally to a "compartmentalization" of functions and tasks within the investigative team. This situation can be turned to advantage with regard to security of information. Limiting the technical adviser's access to sensitive case information to only those areas in which his or her expertise is needed should prove easier to accomplish in such large investigations; nevertheless, this principle is an important one in any sensitive case, regardless of size. Internal staff discipline and discretion on the part of the law enforcement members of the team, coupled with physical data and file security precautions, are critical concomitant aspects of a successful need-to-know information access policy.

Serious consideration should be given to the value of segregating elements of a major complex investigation. This remains true with computer related crime investigations, especially in the situation where a confidential "insider" source of information may be providing intelligence on a continuing basis from within the corporate structure or computer environment itself. Under these circumstances, where there is some evidence to suggest a continuing criminal misuse or abuse of the computer and the total scope of the investigation is not yet clear, the identity and perhaps even the existence of the source should be safeguarded from anyone without a clear need-to-know. This is especially true where the source himself has asserted this right for fear of retaliation and where the consultant may only have a short-lived involvement or responsibility in connection with the case.

5.4.2 Utilizing Multiple Experts As A Cross-Check on Each Other

The more sensitive and/or unique the input which a technical adviser is contributing to the investigation, the greater will be the danger of placing uncorroborated reliance on that information in erecting the investigative and prosecutive theories. Moreover, the greater will be the possibility in such instances that efforts to compromise or neutralize the expert--illicitly, as through bribes, or legitimately, as through defense efforts to impeach credibility--will occur.

Whenever the facts and circumstances, coupled with available human and fiscal resources, permit, multiple sources of expert input should be sought. Especially on very sensitive or pivotal issues in the case, a "second opinion" provides an excellent quality control as well as security precaution.

Under some circumstances, it will prove more advantageous to let each expert know that another source for such input is also being utilized. Disadvantages from this approach, however, are potentially great: Likely alienation of the consultant, increasing the possibility for collusion between the experts, and lack of cost effectiveness are some possible disadvantages here.

5.4.3 Reliance on Technological Aids

Depending upon the procedures of each prosecutor's office and applicable State laws, some units may consider the administration of a polygraph examination as an adjunct to, but not a replacement for, other traditional background investigation techniques. Each situation will be different and, obviously, any advantages must be considered and balanced against potential problems in the developing relationship with the consultant. It is strongly recommended that a waiver be obtained if a polygraph is used and that surreptitious means such as the voice stress analyzer not be employed. If a surreptitious analysis is performed, aside from the obvious legal and ethical implications, a sense of antagonism and distrust will have been created within the investigative team. This must be avoided. Security checks are legitimate and should not create problems if accomplished in a professional and straightforward manner.

5.4.4 Deputizing the Expert

Under exceptional circumstances, such as when access to very sensitive materials will be required, the law may dictate that only law enforcement officers have access. Examples of this could be disclosure of an ongoing court order for electronic surveillance or access to secret grand jury proceedings. Under these circumstances, consultants/experts may have to be specially deputized. They should be advised in writing, and required to acknowledge receipt of such notice in writing, so that they understand the legal sanctions against unauthorized disclosures (often criminal penalties). In addition, for persons without previous experience in these areas, it may be desirable, simply for the increased sobering effect, to take such a special deputy before a judge and have the court enter an order reinforcing the prohibition against premature or unauthorized disclosure.

Very often the solemnity of these proceedings alone is enough to serve as an effective reminder for the inexperienced, especially when coupled with a precaution concerning potential contempt of court proceedings if the precautionary order were to be violated. This could be overdone and traumatize the new member of the team, but if done properly, it can have quite the opposite effect of amplifying the professionally serious nature of the investigation. From a practical psychological standpoint, it can be helpful for the purpose of creating the feeling with the new team member consultant that he or she is engaged in something very special and is now accepted on the "inside," with all of the accompanying privileges and responsibilities. Obviously, some personality types will respond more favorably to this approach than will others and the conversion of experts into special deputies must proceed cautiously.

The process of deputizing outside individuals, albeit technical experts working hand-in-hand with career law enforcement professionals on the case, could precipitate legal problems in some jurisdictions. This practice must therefore be employed cautiously and only after a complete legal analysis of the implications. Possible legal complications arising from the practice of deputizing technical advisers include the following:

- The Federal Government and several of the States have statutory prohibitions on the books against employing a private detective to enforce public laws.[1] Deputizing a private security consultant, for example, who might then participate with career law enforcement officials in the drafting and serving of search warrants, crime scene search, and/or interrogations of witnesses would arguably violate such "Pinkerton Law" provisions. Possible exclusionary rule problems and sovereign immunity problems could as a result arise for both the investigative agency and the deputy, either in the context of the case at hand or later, in a separate suit.

- Most States have standards for law enforcement officer certification and procedures for obtaining such certification, by virtue of courses of education and training, etc., which are embodied in statute or regulations. Deputizing private individuals who do not otherwise meet the State standards for law enforcement officer certification could also lead to legal implications later on.

The role of the particular expert witness in a given case will, as noted earlier, dictate the advisability of deputizing him or her. The above caveats may or may not bear on the decision, depending on the role the expert will play (or be limited to playing) and the state of the law in the jurisdiction.

5.5 Weighing Credibility Factors

Frequently, key technical advisers or prospective expert witnesses will display one or more personal history problems, credentials problems, or personal idiosyncracies that will, if known to the defense, have a potentially negative impact. The decision whether to utilize the adviser and/or designate him as an expert witness despite such problems must be the result of a subjective but dispassionate weighing of the impact on credibility.

What kinds of negative personal history discoveries will have more bearing on the credibility of the expert than others? The answer to that question will vary greatly, depending on a number of facts. What follows illustrates some of these. Remember we are at this time primarily concerned with the factor of credibility. Let us suppose that in the course of the background investigation or preliminary interview, it is discovered that, when much younger, the expert was once arrested for possession of a small amount of marihuana (20 years ago while he or she was in college). The impact that this will have on a judge or jury regarding the credibility of the expert as an expert witness will vary considerably from one geographic region of the country to the next, and even between urban and rural settings within the same State. Generally speaking, though, this matter will have far less negative impact on the witness' credibility than would certain other happenings which were not criminal offenses.

Let us suppose that, more recently (five years ago), the expert was expelled from graduate school for cheating on an examination and one year later was civilly sued, successfully, for breach of contract in the writing of a book in which certain key materials were plagiarized. To make matters worse, an important element of the prospective expert's professional reputation may have been based on the book. Now, in the first instance, where there was an arrest for a violation of criminal law but no conviction, a judge or jury might not attach too much negative weight to a 20 year-old incident of that type, assuming there was no additional drug abuse in the intervening period. On the other hand, the second incident, more recent, though noncriminal in nature, would probably have more of a damning impact on the credibility of such an expert since it affects integrity and professional reputation, especially of a potential expert witness. The first example might be more likely to be discovered and yet the second example, administrative and civil in nature, might be the more significant and relevant to the issue of credibility.

5.6 Establishing Security Within the Investigative Unit

Several key privacy and security protections have been suggested in previous sections of this chapter which have generic applicability to all computer related crime cases, whether large or small, complex or simple. The value of a number of these as general management tools is also discussed in Section 7.0, below. By way of summary, it is suggested that the following steps, at a minimum, must be taken to insure security within the investigative/prosecutive unit for any computer related crime case:

- limit access by outside experts to documents and other data gathered in the course of the investigation on a need-to-know basis;
- execute a written agreement with the expert which defines the nature and scope of his or her role;
- obtain a signed notice from the expert that he or she is aware of the privacy and security requirements in force in the investigative unit, agrees to comply with them, and understands the possible penalties for breaches of security;
- clearly define the chain of command within the unit and designate a particular law enforcement professional as the expert's contact; specify the nature and scope of the contact's authority to guide and direct the activities of the expert;
- maintain ongoing monitoring of the expert's activities and contacts during the course of the investigation, pursuant to a combination of means which are ethical and of which the expert has been apprised; and

- conduct periodic security checks during the course of the case to provide follow-up and update to the initial reference checks.

5.7 Positive Approaches Toward Preventing Breaches of Security

At the same time that the above precautions are instituted to guard against breaches of security, positive interpersonal steps should be taken to maintain team loyalty and prepare outside experts for the pressures and frustrations of a major case, thereby working to prevent breaches of security from arising. This section suggests several such techniques.

Try in every way possible to keep the relationship between team members positive and constructive. This in itself will minimize the occurrence of security breaches and leakage of information either to the media or the suspect individuals or organizations. Perhaps one of the most common security problems in protracted white collar crime investigations is the "frustration leak" of case related information. Maintaining team morale and loyalty can counter this tendency.

Psychologists have now demonstrated through research that one of the best ways to deal with frustration and job stress is to simply understand beforehand what it is, how it occurs and what to do about it once the indicators begin to appear. Persons outside of the criminal justice system often do not understand the delays and cumbersome procedures that are part of our system of law. They should be oriented in this regard as the case develops, or at some point they may throw their hands up in futility, or inadvertently compromise the case in some fashion by inappropriately venting their frustrations. This is a particularly acute hazard in those types of cases that frequently go on for months, or years, with questionable outcomes in terms of sentencing and deterrence.

Those experienced in white collar crime investigations and prosecutions have often heard victims and witnesses say after a long and drawn-out trial, "Never again." Prepare your consultants and expert witnesses for this experience beforehand, without imparting a negative or cynical tone to the case. If things turn out a little better, let everyone be pleasantly surprised for a change.

As much as possible, be specific and flexible in developing the contract with the consultant/expert. This document should also contain some specific elements relating to security requirements and procedures. Specify the satisfactory completion of a background investigation before the contract is finally negotiated, perhaps also including a provision for obtaining a fidelity bond, if deemed advisable. Finally, security and integrity monitoring of all team members must be a continuing process with fixed accountability and responsibility. Do not conduct background checks and then go to sleep on the issue of security over the course of a lengthy, complex and often frustrating computer related crime investigation.

5.8 Legal Remedies for Breaches of Privacy or Security by An Expert

Privacy issues will mainly arise in a computer context insofar as the law recognizes certain information which may be contained on computers is confidential and affords legal protection against its misuse. The basis for such protection may be statutory, common law and/or constitutional. The information protected may pertain to individuals, to businesses (proprietary information), or to Government itself (e.g., national security information). Privacy consideratons give rise, in turn, to considerations of computer security, to the end of safeguarding computer systems and the integrity and confidentiality of information contained therein.

The use of expert witnesses/consultants and their usefulness in computer related crime cases is the focus of this Manual. It is the privacy and security considerations legally attendant upon such use which will be addressed here. These considerations are a consequence of the access afforded such experts during the course of an investigation or trial to computer systems and confidential computer information. This section addresses five such forseeable consequences. These are as follows:

- illegal acts against a computer or its software;
- misuse of confidential information;
- unlawful out-of-court disclosures;
- breaches of special privileges (e.g., attorney-client privilege); and
- violations of specific computer security laws.

These general areas of possible law violation and legal remedies available to counter such actions by experts are illustrated in Table 11, below.

Table 11

Federal and State Causes of Action For Breaches of Privacy or Security by Computer Crime Consultant/Expert Witness

ILLEGAL ACTS AGAINST A COMPUTER OR ITS SOFTWARE WHICH IS EVIDENCE IN A CRIMINAL CASE:

- Embezzlement of public money or assets
- Theft of Government property or records
- Malicious mischief/destruction of property
- Concealment/removal/mutilation of court reports or records
- Criminal trespass

MISUSE OF CONFIDENTIAL INFORMATION FOR ONE'S OWN GAIN:

- Prohibitions against "special Government Employees" using inside informaiton for private gain
- SEC Rule 10b-5 (securities violation)
- State securities laws

UNLAWFUL OUT-OF-COURT DISCLOSURES:

- Federal statutes
  - National Security Act
  - Trade Secrets Act
  - Privacy Act
  - Census Act
  - IRS Code of Confidentiality
  - Fair Credit Reporting Act
  - Right ot Financial Privacy Act
  - Family Educational Rights and Privacy Act
- State statutes
  - medical records
  - education records
  - tax records
  - arrest records
- Tort Liability
  - defamation
  - invasion of privacy
  - violation of trade secrets
- Breach of Contract

BREACH OF SPECIAL PRIVILEGE:

- Prohibition against unauthorized release of Government reports by employees
- Theft of military or State secrets
- Attorney-client privilege
- Privilege against disclosure held by party to litigation

VIOLATION OF SPECIFIC COMPUTER SECURITY STATUTES:

- Removal of classified national security information from Federal computer
- State statutes banning computer abuse

5.8.1 Illegal Acts Against a Computer or Its Software

The most obvious, though presumably least likely, risk in the access afforded an expert to computer hardware or software during the course of a case is the commission of illegal acts by the expert upon the equipment or physical evidence which derives from a computer (i.e., magnetic tape or printout). These may include destructive acts against the system and/or the destruction, theft or alteration of information contained therein.

Such acts constitute what is commonly understood as computer crime. The various traditional legal provisions which may be brought to bear upon such acts are extensive at the Federal and State levels and are addressed in a companion publication. These include, by way only of illustration, statutory provisions such as those to prohibit embezzlement and theft of public money, property or records; malicious mischief upon Government property; and concealment, removal or mutilation of court records and reports. In addition, it should be noted that several States have specific computer related crime statutes on the books which could be invoked in such situations.

5.8.2 Misuses of Confidential Information

It is the law in the Federal system that agency regulations contain a provision to the effect that no "special Government employee" may use inside information obtained as a result of his Government employment for private gain.2/ Some States have similar provisions on the books. A "special Government employee" has been defined by statute as:

> (A)n officer or employee of the executive or legislative branch of the United States Government, of any independent agency of the United States or of the District of Columbia, who is retained, designated, appointed or employed to perform, with or without compensation, for not to exceed one hundred thirty days during any period of three hundred sixty-five consecutive days, temporary duties either on a full time or intermittent basis...3/

An individual who entered into an agreement with the U.S. Justice Department to appear as a fact witness at a criminal trial and to serve as an adviser to the prosecution has been deemed a "special Government employee."4/ Whether there are expert witness/consultant roles not encompassed by the statutory definition is not clear from existing law.

A more narrow form of misuse of confidential information by an expert witness/consultant may entail potential liability under the law. Rule 10b-5 of the Securities and Exchange Commission

(SEC) makes unlawful the perpetration of fraud upon any person in connection with the purchase or sale of any security.[5] The SEC in a 1961 decision stated that one who has access, directly or indirectly, to information intended to be available only for a corporate purpose may not take advantage of such information knowing it is unavailable to those with whom he is dealing.[6]

The Second Circuit Court of Appeals in 1974 considered an action brought against a corporation's underwriter, which had lawfully been privy to confidential information from the corporation's directors that a sharp downturn in earnings was anticipated. The court held the underwriter liable on disclosing the information to its customers, and its customers possessing that confidential corporate information liable on trading in that corporation's stock.[7] The Supreme Court, in a very recent (and its only) opinion directly addressing insider trading, noted with approval these and related cases establishing liability, while overturning a criminal conviction.[8]

Such are the parameters of the law bearing upon the potential liability of an expert witness/consultant for the misuse of confidential information under SEC Rule 10b-5. Where in the course of an investigation or prosecution an expert is given access directly to a corporation's computer records, disclosure of material confidential information, or trading in that corporation's stock with such information may constitute liability. Trading in other stock on that basis would be more problematic, as would disclosure or trading on the basis of confidential corporate information acquired by the expert through access to governmental computer systems. The latter situation raises the issues addressed in part in Section 5.8.5, below.

5.8.3 Unlawful Out-of-Court Disclosures

The largest single problem area encountered in breaches of privacy by outside experts involves unauthorized disclosures. Possible remedies here include criminal prosecution (or civil suit) under Federal or State statutes or by virtue of State tort or contract law.

5.8.3.1 Federal statutes

An out-of-court disclosure by an expert witness/consultant may be unlawful because the disclosure is in violation of a Federal statute. One needs to ask in each instance whether the specific information disclosed is of a type the disclosure of which is prohibited by the statute; whether the specific type of disclosure (i.e., to whom and for what purpose) is permitted by the statute; and whether one in the role of expert witness/consultant is governed by the statute's liability provisions.

Several Federal statutes designate information as confidential, and prohibit such information's disclosure. Whether a given statute makes unlawful disclosures by an expert witness/consultant again would appear to depend upon whether the statute's liability provisions reach one in such a role.

The answer is affirmative as regards national security information. The disclosure of classified information is prohibited by statute, with criminal penalties applicable to "whoever knowingly and willfully communicates, furnishes, . . ."[9] The photography, mapping or other representation of military defense properties is, likewise, prohibited by statute, with criminal penalties applicable."[10]

By contrast, unlawful disclosures under the Trade Secrets Act are subject to criminal penalties applicable only to "any officer or employee of the United States or of any department or agency thereof."[11] Criminal penalties under the Privacy Act of 1974 similarly make reference only to "any employee of an agency."[12] Whether expert witnesses/consultants--ordinarily "special Government employees" by statutory definition--are to be deemed officers or employees for purposes of either statute's criminal penalties is not definitely clear. There have, significantly, been no prosecutions of any kind under either Act. The Privacy Act does make provision for civil liability as well; only agencies, however, are subject to such civil actions.

Two more specific confidentiality statutes are the Census Act[13] and the recently enacted Internal Revenue Code on Confidentiality.[14] The Census Act provides criminal penalties for unlawful disclosure of individual census reports, and permits access only for census purposes and only to sworn officers and employees of the Commerce Department. The Internal Revenue Code on Confidentiality's criminal penalties for unlawful disclosure of taxpayer return information have reference, in pertinent part, to "any officer or employee of the United States...or any former officer or employee." Civil actions are authorized against any person knowingly or negligently disclosing return information in violation of the Act's provisions.

Statutes such as these govern the confidentiality of records held by the Government. A very few statutes, of recent origin, provide for the confidentiality of certain types of records held by the private sector. The Fair Credit Reporting Act contains criminal penalties for unauthorized disclosures by officers or employees of consumer reporting agencies.[15] The Family Educational Rights and Privacy Act provides for termination of Federal funding on the failure by a school district or college to limit outside access to student records.[16] The Right to Financial Privacy Act allows a customer, whose financial records have been disclosed in violation of the Act, to sue the Federal agency or department or the financial institution responsible for the

READEX FICHE best copy available

disclosure.[17] The only individual liability stipulated by the Act is disciplinary action by the Office of Personnel Management against a Federal officer or employee found to have willfully or intentionally violated the Act.

5.8.3.2 State statutes

An out-of-court disclosure by an expert witness/consultant may also be unlawful, if the disclosure is in violation of a State statute. State informational privacy statutes vary greatly in their object and scope. A given statute may address, for example, medical records, educational records, tax records, or arrest records. A statute may govern Government-held records and/or records held in the private sector. Limits upon disclosure will vary, as will the nature and scope of liability. Whether an out-of-court disclosure by an expert witness/consultant is unlawful as a violation of a State statute will depend upon the same considerations as applied to examination of Federal statutory violations. A compilation of selected State informational privacy provisions appears as Appendix D to this Manual.

5.8.3.3 Tortious liability

An out-of-court disclosure by an expert witness/consultant may be unlawful regardless of Federal or State statutes. Non-statutory civil remedies may be available. One body of the common law is tort law. A tort is conduct, other than breach of contract, which injures another and upon which the law will permit the one injured to sue for damages. Not all injurious conduct, of course, is unlawful. Three torts are especially relevant to an out-of-court disclosure of confidential information by an expert witness/consultant. These are defamation, invasion of privacy, and disclosure of trade secrets.

The essence of defamation is injury to reputation. There are two varieties of defamation--libel and slander. Libel is defamation by means of writing, a picture, an image, or the like; slander is defamation by oral or sign language. For there to be defamation there must be (1) a false and defamatory statement; (2) communication of that statement to a person other than the one suing; and (3) fault, amounting to at least negligence, by the one being sued. The defendant in a defamation suit must have been at least negligent in ascertaining the truth or falsity of the statement and in allowing it to be communicated. For certain forms of slander a plaintiff must show concretely how he or she has been injured; otherwise, so long as the elements of defamation have been satisfied, harm will be assumed.

The concern here is out-of-court, or more broadly, non-judicial disclosures by an expert witness/consultant. A witness is absolutely privileged to make defamatory statements concerning another in communications preliminary to a proposed judicial proceeding or as a part of a judicial proceeding in which he is testifying, if it has some relation to the proceeding.[18] A witness' statement, made under oath in open court in response to a question on cross-examination, that the plaintiff was a "crook," was held immune from suit for defamation.[19] In another case a written report prepared by a psychiatrist, at the request of a wife's attorney, concerning the alleged sexual abuse of her sons during visits with their father was held related to pending divorce proceedings, and thus immune from suit for defamation.[20] By comparison, an attorney's statement to the managing editor of a newspaper that his client, who was awaiting trial on charge of rape, denied the charge and said the woman had submitted to his advances willingly, was held outside the scope of immunity, and open to suit for slander.[21] The critical fact in that case was that the statement was made to persons in no way connected with the judicial proceeding.

The second tort for consideration is that of invasion of privacy. While defamation is concerned with injury to reputation, invasion of privacy concerns interferences with an individual's right to be let alone, and resulting injury to feelings. Most States today recognize this tort action by case law; some States do so by statute. A few States do not recognize it at all. There are generally considered to be four forms of invasion of privacy. Only two, however--the public disclosure of private facts, and depicting one in a false light--are relevant here.

For the public disclosure of private facts to constitute an invasion of privacy, (1) it must be characterizable as highly offensive to a reasonable person; (2) the information must be truly private, and (3) the information must be publicized. The information must be truly private; matters of public record and public occurrences do not qualify.[22] Communication to a single person other than the plaintiff is sufficient for defamation. However, invasion of privacy requires communicating to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. Unlike defamation, a statement may be true and its public disclosure, nonetheless, constitute an invasion of privacy.

For placing another in a false light to constitute an invasion of privacy, (1) it must be characterizable as highly offensive to a reasonable person, and (2) the one doing so must know he is portraying his subject in a false light, or must act in reckless disregard of the issue. This is distinguishable from defamation in that, while the portrayal must be contrary to fact and highly objectionable, it is not necessary that it have held its subject up to ridicule.

The third and final tort for consideration is the unlawful disclosure of trade secrets. A number of States have criminal statutes prohibiting the disclosure of trade secrets.[23] For purposes of tort law, whether a disclosure constitutes an unlawful disclosure of a trade secret depends upon whether the information constitutes a trade secret, and the means by which the discloser has come upon the information. A trade secret is generally information which is not publicly known, and which affords a competitive advantage to the business entity processing it.[24] A trade secret is protected only against those who "discover" it by improper means, but the protection will last infinitely so long as secrecy is maintained. The Supreme Court in a recent opinion characterized the doctrine of trade secrets as guarding "the very life and spirit of the commercial world."[25]

The Restatement of Torts identifies four bases for liability, one of which is especially relevant to a disclosure by an expert witness/consultant. That is where one who discloses a trade secret, in doing so, breaches a confidence, reposed in him by the other in disclosing the secret to him.[26] The Restatement, in its comprehensive rationale for the tort of trade secret disclosure, states that the theory that has prevailed is that the protection is afforded only by a general duty of good faith and that the liability rests upon breach of this duty; that is, breach of contract, abuse of confidence, or impropriety in the method of ascertaining the secret.

5.8.3.4 Breach of Contract

Sections 5.6 and 5.7 recommend that the expert witness/consultant in a computer related crime case be put under written contract, and that specific provisions against unauthorized disclosure of sensitive data to which the expert gains access during the course of a case be included in such a contract. Assuming that the Government's expert has entered into such a contract at the outset of his relationship to the case, a civil suit for damages for the breach of any privacy and security of data provisions of the contract could be instituted. A more direct recourse here would, of course, be to withhold payment to the expert witness/consultant and cancel his or her contract if the breach of security becomes known while the relationship still exists, i.e. before the case is closed. Any action for breach of contract could also seek to recoup monies already paid out to the expert witness/consultant who violated the contract by breaching its privacy and security provisions.

5.8.4 Breaches of Special Privileges

The role of the expert specifically as witness raises issues of a further dimension. The law recognizes in certain situations a privilege whereby a witness may refuse to testify, or may be prevented by another from testifying, as to certain matters. (Privileges relating to attorney-client or husband-wife communications are among the better known.)

Reports required by the Federal Government are generally privileged, on the basis of a privilege written into the statute requiring the report.[27] A court will ordinarily consider the subject matter of a statute, and the policy underlying a statutory privilege. It may regard a given privilege as absolute or qualified, and if qualified, may proceed to balance interests in confidentiality against interests in disclosure. A given statute may provide merely that the Government not publicly disclose the reported information; it may designate information as confidential except for court order; it may prohibit its disclosure in any trial; or it may limit disclosure to instances in either the submitter's or the public's benefit.

Whether trade secret information will be privileged is usually determined by a balancing of interests. The Supreme Court's draft of the present Federal Rules of Evidence recognized trade secret privilege only where doing so would "not tend to conceal fraud or otherwise work injustice."[28] A court, if it chooses, may utilize any of various forms of protective disclosure, such as appointing a master, appointing an independent expert, revealing material only to the judge or trial examiner, omitting material form the record of the case, or disclosing material to the other attorney, but not to the other party.

Military and state secrets are privileged. One may compare the approach taken to various aspects of this privilege in the original draft of the Federal Rules of Evidence,[29] the subsequent Supreme Court draft of the Federal Rules of Evidence,[30] and the case of United States v. Reynolds.[31]

The attorney-client privilege also has a bearing on expert witness privilege. When an expert is not intended to be called as a witness, communications to the expert by the client or by the attorney regarding the client in the Federal system are privileged, for the reason that the expert is seen as acting as an agent or representative of the attorney.[32] This is not always the case under State law, however.[33]

Certain privacy considerations arise in connection with the role of an expert as such. Parties to a case are permitted discovery of information held by other parties according to and within specified rules. The Federal Rules of Civil Procedure set forth special limits to the discovery of facts known and opinions held by experts.[34] The Federal Rules cover reports, memoranda, or other internal documents by Government agents in connection with the investigation or prosecution of the case.[35] The Federal Rules of Evidence specifically address expert testimony in several rules. Rule 702 states that, "[i]f scientific, technical, or other specialized knowledge will assist the trier-of-fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion or otherwise." Rule 612, applicable to all witnesses, permits the court in its discretion to make available to the opposing party writings used by a witness prior to trial to refresh his memory for the purpose of testifying. The expert witness may thus become the conduit to information otherwise not available. In one case the court ruled that whatever privilege may have been attached to certain material had been waived by previously furnishing the material to an expert witness, though not as a basis for testimony or as a memory refresher, but merely as general background.36/

5.8.5 Violations of Specific Computer Security Laws

Legal provisions for computer security are few and of very recent origin.37/ Such provisions may concern administrative, technical or personnel practices. It is the personnel safeguards that are chiefly of concern here. Notwithstanding whatever degree of risk there may be in the utilization of an expert witness/consultant, the law under only very few circumstances requires that any security measure be taken prior to an expert's being afforded access to computer records. One exception is classified national security information, access to which necessitates security clearance.38/ The Office of Personnel Management in November 1978 announced specific criteria and amplifying guidance for the purpose of conducting investigations and designating positions associated with Federal computer systems into its existing personnel security program.39/

As noted previously, several States have recently enacted specific computer abuse/crime statutes. The unauthorized physical penetration of a computer, under certain of these statutes, is itself a crime.

blank page

6.0 UTILIZING THE EXPERT IN ALL PHASES OF THE CASE

Each computer related crime case will be unique. Facts and circumstances will vary from case to case and the applicable law will vary between jurisdictions. The need for outside technical assistance will vary in response to these factors. The availability of outside experts and the fiscal constraints under which the investigation must operate will likewise be major factors in shaping the configuration of outside expert assistance applied in a given case. The purpose of this Section is to suggest general areas where outside expertise can prove useful.

6.1 Preliminary Investigative Work

For traditional, "reactive" law enforcement agencies faced with a computer related crime, outside technical advisers will usually be utilized at the investigative stage on an informal, ad hoc basis. At this earliest phase of a computer related crime investigation, the investigative team will be primarily occupied with seeking to clearly understand the nature of the case; determine whether a violation of law has occured; identify perpetrators; analyze the system; and locate/preserve evidence. This level of assistance may not require a formal contract or paid services until such time as a more protracted relationship may be indicated and the precise nature and extent of the case is known. Often adequate temporary expertise can be located within vendors or victim firms, universities or vocational school staffs, or even certain professional consulting firms willing to do a certain amount of voluntary "front end" work in the hope of obtaining a new contract for services, or perhaps expanding existing contracts with other, related governmental agencies or departments.

The possible roles for outside technical advisers at the investigative stage of a computer related crime case are much greater in the "proactive" sort of investigative unit or department described in Section 3.2, earlier. As has been noted, proactive white collar crime units will often commence major investigations in advance of the filing of complaints rather than after, as is the case with the reactive mode. Indeed, the proactive approach to major crimes investigations generates the complaint, rather than the other way around. This approach, whether in a computer related crime case or otherwise, will tend to encompass the use of one or more of the following added dimensions:

- the intensive surveillance of persons or places, whether by human or technological means, in order to detect patterns of suspicious activity;

- the extensive use of confidential sources, paid informers, and/or undercover officers to gather especially sensitive criminal intelligence data;

- the periodic monitoring of bank accounts, credit sources, etc. on persons suspected of ongoing embezzlement or other fraudulent schemes;

- the extensive use of investigative grand juries, coupled with selective grants of immunity to induce testimony; and

- the planning and implementation of "Operation Sting" type tactics to precipitate criminal action in a controlled environment from a certain group of suspects.

In each of these areas of proactive investigations, the need for the services of technical advisers from a wide variety of fields--whether loaned, gratis or compensated--is great. Of course, the type of expert skills needed will vary with the facts and circumstances of the case. As a general rule, proactive investigations will obtain a "handle" on the nature and extent of the crime much earlier in the process, thereby precipitating earlier and more extensive use of outside expert services. Table 12 illustrates the many steps in the investigative stage at which expert assistance could be employed.

6.2 The Pretrial Stage

Under a distinction usefully drawn by the U.S. Supreme Court [1/] the "investigative stage" of a criminal case, dominated by the police, is generally considered to draw to a close and the "pretrial stage," dominated by the prosecutor, commences when one or more of the following occurs:

- the Government has narrowed its investigation to the point where it has focused on one or more particular suspects;

- the attorney for the Government has decided that the public interest will be served by initiating a prosecution; and/or

- the prosecutor files a criminal complaint with the court.

During this phase, the outside technical adviser can play an equally important role. By and large he or she will now be working for, and in direct support of, the prosecutor's office (though case management by the prosecutor at the earlier, inves-

Table 12

Areas for Possible Technical Assistance at the Investigative Stage

- Detecting the crime.
- Advising whether facts and circumstances, local law will support a charge of law violation.
- Developing an overall theory of the case.
- Preparing mission paper as background justification to preliminary investigation.
- Conducting feasibility study in advance of preliminary investigation.
- Conducting cost benefit analysis in advance of embarking on major case investigation.
- Advising on patterns of known computer abuse in a given industry.
- Profiling computer felons in a given industry from prior cases and unreported incidents.
- Providing technical assistance in setting up scenarios for "operation sting" activities.
- Serving as undercover member of law enforcement team.
- Operating complex technological surveillance equipment.
- Providing sensitive "insider" information to the Government
- Performing financial monitoring/credit checks on suspect's accounts and analyzing findings.
- Testifying before investigative grand juries.
- Conducting investigator orientation sessions on basics of computer processing and its applications in victim's industry or field.
- Assist, on-site, with crime scene analysis.
- Advise on methods of obtaining complex evidence intact (e.g. "dumping the program").
- Interpreting complex data and physical evidence.
- Preparing search warrants and subpoenas.
- Indexing case intelligence and subpoenaed evidence.
- Advising on techniques of evidence preservation and storage.
- Explaining intricacies of victim's operations.
- Explaining applications/vulnerabilities of victim's hardware, software.
- Conducting external EDP audit of victim organization.
- Advising on gaps in physical plant and data base security at victim's location.
- Constructing probable modus operandi.
- Preparing technical questions for preliminary interviews of witnesses/depositions.
- Focusing on the suspect(s), advising on probable means, motive and opportunity.
- Preparing intelligence bulletins for staff on new developments in the case.

tigative stage may have already occurred under the multi-disciplinary team approach to major case investigations recommended in Section 1.2, above).

It can be expected that as the case moves from the investigative to the pretrial stage, additional experts of different types will be added to the Government team. The roles of others--those involved at the earlier phase--will change at this stage. For example, behind-the-scenes technical advisers may become potential expert witnesses. Again, the facts and circumstances of each case will dictate both the kinds of outside expertise required and the roles those experts will play in the case.

Table 13 presents a listing of likely areas in which outside technical assistance could prove helpful at the pretrial stage in a computer related crime case. As this illustrates, planning trial strategies, analyzing and interpreting the physical evidence, preparing expert testimony and assisting the Government to interrogate or depose witnesses are key functions at this stage which will involve outside technical assistance. These and other pretrial functions will center around the pretrial conferences, at which trial attorneys, experts, and the senior investigators who "broke" the case prepare and build the trial strategy.

6.3 Litigation Support and Expert Testimony

Prospective expert witnesses who have been performing in the role of behind-the-scenes, "informal" technical advisers to the prosecution at the pretrial stage will make the role transition to that of expert witnessses once litigation commences. Other advisory functions in support of the Government's case in chief may also be performed at this phase by outside technical advisers--whether by those who will take the stand as expert witnesses themselves or by other specialists, who will continue to remain behind-the-scenes--as the facts and circumstances of each case dictate. Table 14 illustrates the likely functions of expert witnesses and other technical advisers at the pretrial stage in a computer related crime case.

Clearly, the main function of the outside expert at this stage of the case will be to provide expert testimony on behalf of his party's case. Such testimony will, as in other cases, commence with a presentation of his or her qualifications by the prosecutor to the judge and jury, followed by an opportunity for the defense to challenge, through cross-examination, (1) the expert's qualifications and/or (2) the expert's competence, bias or financial interest in the outcome of the litigation.2/

Once the expert's credentials have thus been proffered to the court, and provided he or she is not disqualified on grounds of competence, bias or financial interest by the defense, the

Table 13

Areas for Possible Technical Assistance at the Pretrial Stage

- Conduct orientation sessions for team prosecutors on computer processing/computer applications in victim's industry
- Advise on victim's operations, equipment.
- Provide confidential "insider" information.
- Serve as an undercover agent.
- Testify before grand juries, at preliminary hearings as an expert.
- Interpret the overall evidence in support of erecting prosecution's trial stategy.
- Advise on drafting search warrants, subpoenas for complex technical matters.
- Analyze the fruits of successful searches and seizures.
- Authenticate the physical evidence.
- Insure proper and secure storage/preservation of the evidence and chain of custody.
- Draft Government discovery motions for complex material.
- Advise on necessity for and extent of compliance with defense discovery motions.
- Advise on choice of laws, meeting burden of proof.
- Anticipate defense strategies/objections in technical areas of one's expertise.
- Check out opposing expert witnesses and advise on their stature, ways to impeach, etc.
- Suggest questions for cross-examination of opposing expert witnesses.
- Devise strategies for getting necessary evidence admitted.
- Prepare to testify as an expert witness.
- Provide general technical assistance to prosecutors at pretrial case conferences.

Table 14

Areas of Technical Assistance by Experts/Expert Witnesses at the Trial Stage of a Computer Related Crime Case

- Prepare for in-court examination on one's own qualifications
- Aid the prosecutor to draft questions for qualifying oneself; provide books to review, etc.
- Prepare exhibits to accompany one's own testimony and/or that of another witness.
- Review one's own lab notes or field notes to facilitate later in-court referral to these as an aid to refreshing recollection.
- Review transcripts of one's own previous testimony in this/other cases, one's publications, etc., to guard against possible inconsistencies or direct examination.
- Familiarize oneselft with the latest developments in one's field in preparation for cross examination/challenges to competence.
- Prepare for cross examination by rehearsals, playing devil's advocate, etc.
- Coach other, less experienced prospective witnesses on courtroom demeanor, techniques for sustaining cross-examination, etc.
- Meet with opposing counsel, if requested, and cleared with prosecutor, prior to testifying.
- Advise the prosecutor on general routine questions/preemptory challenges, etc.
- Assist prosecutor with drafting opening statement.
- Advise the prosecutor on how to effectively challenge the competence/qualifications of opposing expert witnesses.
- Co-chair the management of the prosecution.
- Provide expert testimony on direct examination on one or more of the following points/issues:
  - for laying foundation for admission of computer evidence (printouts, etc.) under Business Records Exception to the Hearsay Rule;
  - for laying foundation for admission of any evidence by showing its authenticity and chain of custody;
  - in answer to hypotheical questions; or
  - in answer to factual questions (including on the ultimate issues in the case).
- Sustain cross examination on one's expert testimony on direct.
- Advise the prosecutor as to questions to ask on re-direct.
- Testify on re-direct.
- Review the program of the case with the prosecutor at the end of each day of litigation and advise on changes in trial tactics, strategy, etc.

role of the expert witness becomes that of presenting his or her expert opinion on particular points being litigated. In the Federal system and many of the States, expert witnesses are no longer limited to testifying in response to hypothetical questions, but may testify directly from their knowledge or opinion on the particular facts at issue in the case.[3] As in other areas of litigation, expert witnesses in computer crime cases will be called upon to testify to the authenticity and chain of custody of the physical evidence, which is a function of laying the foundation for admission of such items into evidence in the case. Unique aspects of the process of obtaining admission of computer records (printouts, magnetic tapes, etc.) into evidence in computer crime cases will also require selected expert witnesses to assist the prosecution, through their testimony, to do the following:

- overcome possible defense objections to the introduction of computer records as violative of the Hearsay Rule; and

- demonstrate that such records were made in the normal course of business and therefore admissible under the Business Records Exception to the Hearsay Rule.[4]

And, of course, at the conclusion of the expert's testimony on direct examination, he or she will be required to undergo cross examination by the defense, followed possibly by re-direct examination by the Government.

The effectiveness of the expert witness' testimony will be directly in proportion to the degree of preparation and rehearsal between the expert and the prosecutor. If the expert is in the habit of providing prosecutors a "standard list of questions" eliciting his testimony, this list must not be utilized as a replacement for preparation. If procedurally allowable, the prosecutor may want the expert to continue rendering assistance by "second chairing" the presentation of the evidence, i.e., advising on means of simplifying presentations of exhibits and testimony by providing examples of how to develop audiovisual presentations in support of the litigation.

blank page

7.0 MANAGING THE EXPERT

The preceding Chapter discussed in detail techniques to effectively use outside experts at key points in the case in order to obtain particular legal results. As such, it addressed investigative and trial strategies and tactics. In contrast, this chapter presents general management considerations, applicable at all stages of the case, which if employed should facilitate the use of outside experts to achieve the overall smooth functioning of the investigation and the production by the expert of whatever work product is required. As such, the considerations presented have equal applicability beyond the computer related crime case to all major case investigations. In addition, many of the principles advanced are sound management techniques useful whenever a contractor or outside consultant is retained to perform any tasks.

7.1 General Management Considerations for All Phases of the Case

Sound management of technical advisers in computer related crime cases will rest on several general principles, regardless of the phase of the case in question, the technical specialty of the expert, or whether it is intended that he or she be used only behind-the-scenes or as an expert witness in court. This Section presents such general management considerations. Section 7.2 will present additional management considerations applicable to expert witnesses only.

7.1.1 Establishing Rapport and An Atmosphere of Trust at the Outset

Once the decision is made to seek outside technical assistance in a computer related crime case and a prospective expert, or experts, have been identified, conscious efforts must be made by the law enforcement personnel on the investigative or prosecutive team to make the expert feel like a professional peer. The atmosphere at the initial contact meeting and later orientation meetings between the investigative team and the expert will be crucial in establishing this sort of necessary rapport with the expert.

As discussed in Chapter 4.0, the identification and selection of experts who are "team players" will make consultant management much simpler. The necessary corollary to this principle, however, is that the expert must be made to feel he or she is an important and accepted member of the team. Maintaining such rapport with the outside expert may prove difficult as the case progresses, due to the need for case security in certain areas, the pressures that will set in for all members of the team at critical junctures, and the often lengthy duration of the more complex cases.

To counter these and other inevitable threats to interpersonal rapport between the expert and law enforcement members of the team, a very thorough briefing of the consultant at the start of the relationship (and perhaps periodically thereafter) is strongly recommended. At such a briefing, specifics should be presented as to the manner in which the investigation will be conducted, the chain of command, the way the Government anticipates using the technical adviser's services, the need for case security, and all financial arrangements, work product specifications and delivery deadlines.

Allowing questions and comments from the consultant as well as requesting maximum input from him or her in shaping these decisions, to the extent practicable, will also go far toward building the essential rapport early. A frank and down-to-earth explanation to the consultant of the problems, pressures and frustrations that can be expected to arise during the course of the case will allow both the law enforcement team and the outside expert to assess whether their anticipated work relationship will be mutually satisfactory.

7.1.2 Integrating the Expert Into the Major Case Investigative Team

Major case investigations can involve ongoing, concurrent activities by a large number of investigators and technical advisers, often in several locations. Maintaining effective overall management of personnel in such cases can prove challenging and difficult. Regardless of the size and configuration of the investigative team, each technical adviser must at a minimum be informed as to the chain of command, the particular person to whom he or she reports, and how he or she is expected to interface with the other members of the team.

Clarity in defining and explaining roles will go far toward keeping the expert "on track" and toward insuring that he or she understands the importance of his or her input vis a vis that of other experts toward the common goals of the investigation. Orientation sessions--at entry onto the team and periodically thereafter--with other members of the team are a useful tool in this regard. In addition, regular, frequent contact with the supervising investigator or prosecutor will insure that the expert is proceeding in his efforts as planned. Regular monitoring and review of the consultant's work product or progress to date on tasks will be a further important check for insuring that the expert and his activities are fully integrated into the overall activities of the team.

7.1.3 Determining, In Conjunction with the Expert, All Facets of His "Negotiated Collaboration" with the Investigation

One very important point that must be recognized early is the fact that professionals, generally speaking, enjoy their autonomy. They are used to being self-directing in their work, and they are commonly skeptical of and resistent toward formally-designated authority figures. This is particularly true when an autocratic form or style of leadership is employed in relationship to management of a staff of professionals. Experts, like others, want to be treated as competent, responsible professionals.

These underlying assumptions lead to the conclusion and recommendation that the philosophy of management for professional teams assembled on a temporary project basis in computer related crime cases be characterized as one of "negotiated collaboration", by which is meant that tasks to be undertaken by the expert be agreed-upon in advance together with deadlines, work products, specifications, and any prohibited actions. Apart from regular reporting, the expert should be allowed to proceed in the performance of his task at his or her discretion, within these previously-articulated limitations. While the particular philosophy of management that prevails in the investigative or prosecutive agency will vary, depending on personal style, standard operating procedures and other factors, it is recommended that in the use of outside professional experts, the management-by-objectives and management-by-exception approaches be used.

To successfully employ the "negotiated collaboration" approach, a detailed statement of the scope of the expert's assignment and the Government's expectations toward its execution and the resultant work product must be agreed upon in advance with the expert. Sections 7.1.4-7.1.7 address particular aspects of this process in more detail.

7.1.4 Determining in Advance the Scope of the Expert's Tasks to Be Performed

Fiscal economy as well as good management dictates that the scope of the expert's tasks be agreed upon in advance, and that the consequent complexity of the work, and anticipated duration of the relationship be understood by all parties. It will not always be possible to anticipate the scope of the expert's work; it will often expand as the case evolves. However, periodic review of the status of the case as a whole and of progress to date by the expert on his or her assigned task should allow for orderly, periodic reassessments of the nature and scope of the expert's needed services.

Often outside input will prove necessary in order to effectively identify, and then articulate to the expert, the planned scope of his or her tasks. Various categories of other technical advisers--such as experienced investigators "on loan" from another jurisdiction, a computer crime scholar who serves as a senior technical adviser to the team, or top management of the victim organization--can be of assistance to the law enforcement professionals in defining the nature and scope of assignments to other, more highly specialized, technical experts.

7.1.5 Fixing Responsibility for Guidance and Direction of the Expert

The larger and more complex the computer related crime investigation becomes, the more personnel are likely to become involved in the case, technical advisers as well as law enforcement officers and prosecutors. Proper supervision and direction of all technical advisers could be a task that would exceed the chief investigator's or senior prosecutor's effective span of control. Delegations of authority and responsibility to junior staff for the control of ongoing efforts by outside technical advisers will as a result often be required.

The larger and more complicated the investigation, the stronger is the need for tight management controls. Establishing a regular contact point within the law enforcement team for each outside technical adviser early on becomes essential in major cases. A clear understanding between all members of the team as to the areas in which direction--as opposed to advice or guidance--is to be exercised over the actions of the expert by the supervising investigator or prosecutor will be critical for the effective and harmonious functioning of the team on the case.

As a corollary to the need for delegating authority and responsibility over the actions of experts, senior case managers must be prepared to back up their subordinates in instances where the expert does not respond to guidance or direction. In such situations, team managers must be careful to distinquish deferring to the expert on technical questions within his or her area of special competence, which is appropriate, from deferring to the expert on issues of case management and control, which could prove disastrous, not to mention demoralizing to the law enforcement professionals on the team.

7.1.6 Agreeing to Level of Compensation, Fee Arrangement, Work Schedule, Deliverables and Payment Plan

A clear understanding in advance between the parties as to the nature and scope of the expert's service must be accompanied by clear understandings as to the expected work products that will be produced and the mode and timing of payment. Disputes over whether the consultant has complied with the requirements as to work products and whether or when payment will issue can be destructive to the ongoing relationship with that particular consultant. Such disputes also can affect otherwise good relations with other experts on the team, and can have a negative impact on the case as a whole by either taking time and attention away from the issues in the case or even by depriving the Government of the work product or testimony of the expert at a critical juncture should the dispute not be resolved.

On the issue of compensation, a daily consulting rate must be negotiated in advance between the consultant and the Government and agreed to by all parties, as noted in Section 4.1, above. Alternatives to the process of negotiating a daily billing rate are, first, entering into an agreement with the expert to perform specified services in return for a fixed fee when the work is completed, or, second, an agreement to pay the expert a fixed fee conditioned upon successful resolution of the case (contingent fee).

The fixed fee contract is an attractive alternative where the length and complexities of the consultant's assignment cannot be fully anticipated at the outset, and/or where available funds are scarce and must be effectively budgeted. The contingent fee approach, while attractive from a cost-benefit perspective, entails certain ethical and strategic problems: American Bar Association standards prohibit the use of contingent fee retainer agreements, as do many State Bar Association rules and other sets of professional standards.1/ In addition, the defense can much more easily impeach the Government's expert witness for bias and/or financial interest where it can be shown that payment to the expert will be directly dependent on his taking the position that will most assist the Government to win its case.2/

On the issue of when payment should be made, the facts and circumstances of the case, standard disbursing policy of the agency, and requirements of the outside expert will be deciding factors. Regardless of what partial payment or lump sum payment plan is agreed to, specifying in advance the dates payment will issue and tying payments to receipt and acceptance of work products are sound management considerations.

With regard to work product, the format, level of detail, etc. of any consultant reports should be spelled out in detail in advance. Requiring the expert to brief his law enforcement contact personnel in advance of writing his report and to submit a detailed outline of its contents for initial review and approval are useful techniques to insure compliance with deliverable requirements and to avoid "surprises" in content, once the work product is delivered, that can affect its utility or credibility.

It is not always possible to determine in advance the time frame required for the outside expert to perform his or her assignment. For some uses of experts, i.e., testifying at trial, the time frame for performance can much more easily be stipulated. Maximizing to the extent possible the practice of requiring expert work products to be delivered by a certain date will go far toward keeping the momentum of the investigation or prosecution effectively in the control of the Government. The team leader must, as a consequence, be prepared to take appropriate corrective action if the technical adviser fails to comply with time deadlines--including withholding or pro rata reducing the agreed upon fee, or replacement of the expert on the team.

7.1.7 Formalizing the Terms and Conditions of the Expert's Utilization In A Written Agreement

Preparing written agreements for consultant services is often viewed by law enforcement personnel as burdensome, unnecessarily cumbersome, and "too legalistic". Yet the advantages that accrue from having the terms and conditions of the agreement for personal services in writing are so great that the time and attention required to reduce the understanding to writing is worth it, even in cases where familiar experts are being used again. Furthermore, the basic terms and expectations in such situations can often be embodied in a simple letter or memorandum of understanding, couched in layman's terms. So long as offer, acceptance and consideration are recited and both parties sign the letter or memorandum, its enforceability as a basic personal services contract will be preserved.

At minimum, such a written agreement should contain the following provisions:

- description of the nature and extent of services to be performed by the expert;
- time frame for performance of services and deadlines for delivery of any particular work products;
- the identity of the official who will provide guidance and direction to the expert and the nature of any supervisory authority vested in that official;
- the level of compensation, payment schedule, and basis on which payments earned are to be computed in return for services rendered;
- stipulation that payment will be tied to formal acceptance of work products, and verification of satisfactory completion of task by a designated official;

- proviso that the Government reserves the right to take certain corrrective action in the event of non-performance or unsatisfactory or late performance;

- indication of how modification or expansion of the agreement so as to add or delete tasks is to be accomplished;

- stipulation as to any regular reporting requirements the expert must adhere to; and

- a stipulation that the expert agrees to keep confidential any information about the case or the identities of those involved in it.

7.1.8 Quality Controls

As noted in Sections 7.1.3, 7.1.5 and 7.1.7, above, building into the consultant relationship effective quality controls over work to be performed is an indispensible facet of any effective consultant management plan. Quality controls will generally consist of two types:

- pre-existing standards and specifications to which the expert's work product must adhere and against which it will be assessed; and

- review and approval authority over the expert's work vested in others, including regular reporting requirements.

It is strongly suggested that quality controls of both types be instituted. The nature of both types should be spelled out in the written agreement with the expert consultant, which clearly lays out both the requirements for quality control with which he or she must comply, and the consequences of non-compliance.

7.1.9 Security Considerations

Section 5.0 details preventive and remedial actions that can be taken by the investigative unit to maintain the privacy and security of data evidence in a computer related crime case. Planning and implementing such security precautions and insuring compliance on the part of outside experts are all aspects of effective case management.

This section will not reiterate the type of security checks and precautions which are discussed in detail in Section 5.0. Suffice to say, informing the prospective consultant in advance about the nature of the security precautions that will be undertaken, the need for instituting such precautions, and the fact that breaches of security will have an immediate impact on a continued consulting relationship is essential so as to preserve an effective and informed working relationship. Embodying a listing of such security precautions in the consultant's contract, or in a separate document which he or she signs, is important in order both to impress upon the expert the seriousness of this facet of the case and to evidence the expert's prior agreement to comply should later corrective action be required.

7.2 Special Management Considerations At the Trial Stage

Several additional management considerations come into play when a technical adviser becomes designated as a "potential expert witness." These factors have to do with proper preparation of the potential expert witness for both direct and cross-examination; readiness for laying the foundation for the advisers' admission as an expert witness; and anticipation of defense objections to the witness testifying or impeachment of the witness who does testify. All of these are appropriate subjects for one or more pretrial conferences between the expert and Government counsel. Convening one or more pretrial conferences in anticipation of expert testimony is an essential aspect of sound case management in preparation for litigation.

7.2.1 Review of the Expert's Views, Writings and Prior Statements for Consistency

In preparation for testifying at trial, both the prosecutive team and the expert in question must carefully review the expert's prior public positions, as espoused in publications, lectures, other consultancies and testimony, etc. for consistency and congruence with the expert's planned testimony in this case. In addition, the planned testimony must be mapped out so that it is consistent with and advances the prosecution's theory of the case. Preferably, a review of the technical adviser's prior public statements should occur even earlier, at the investigative stage when first brought into the case, in anticipation of his or her possible use as a Government expert witness, or as a subpoenaed defense witness. Any deliberate changes in stated views over time on the issues in question, or any inadvertent inconsistencies in views as expressed in different publications or statements must be identified and a contingency plan devised for reconciling the discrepancies, or explaining the reasons for the change in opinion, should these arise on cross-examination.

7.2.2 Review of the Expert's Credentials and Views in Preparation for Laying the Foundation

Counsel for the Government must thoroughly familiarize himself or herself at the pretrial stage with all of the experts' relevant credentials, in preparation for proffering the expert to the court as an expert witness. Obviously, the best (though not the only) source of information on the potential expert witness' accomplishments and qualifications is the expert witness himself. In addition, counsel should personally read the expert's publications, to the extent possible, in order to familiarize himself or herself for the proffer of the expert's credentials as well as for direct examination of the expert witness.

The potential expert witness, conversely, must make a special effort to not only review his or her prior publications and other public statements on the issues in contention, but also review other literature in the field and insure familiarity with the latest technological developments. In addition, the expert should carefully review his or her lab notes, or other notes made in the regular course of research or review of the evidence in the case, in anticipation of the need to refer to such notes while on the stand to refresh his or her recollection, a procedure that will also, incidentally, make such notes discoverable by the defense.3/

7.2.3 Rehearsal of Expert Testimony to Be Given on Direct Examination

Between the time that a technical adviser is designated or selected as a potential expert witness and the time he takes the stand to testify, one or more "full dress" rehearsals of the questions that the Government will ask on direct examination and the answers which the expert witness will give must take place. The more lead time available, the more complex the testimony, and the more critical the expert's testimony will be to the prosecution's case, the greater the number of such rehearsals that should be scheduled.

The prosecutive team should take pains to acquaint the expert witness with any idiosyncracies or predilections of opposing counsel and of the presiding judge, and, if possible, a profile of the jury once impanelled.

Such practice sessions should concentrate on appropriate courtroom demeanor and nonverbal communications skills as well as on the substantive content of the expert's remarks. In addition, the prosecutive team should tape the mock testimony for later review and for use as a learning device for refinements and improvements in both content and delivery in later reherasals.

The prosecutive team should not make the mistake of dispensing with such rehearsals in instances where the expert witness has testified in court before, even on the same subject. The facts and evidence in each case are unique, and these shape the testimony. Just as the prosecutor should require the expert witness to participate in one or more such rehearsals in preparation for direct testimony, the expert should press the often over-burdened prosecutors to sponsor such a pretrial rehearsal where the Government has not taken the lead.

7.2.4 Preparing the Expert Witness for Cross Examination

Similar to the activities recommended in Section 7.2.3 with regard to preparing the potential expert witness for direct, but of even greater importance, is the need to prepare him or her for cross-examination. Many witnesses who convey on direct examination that they are knowledgeable and articulate cannot hold up under vigorous cross-examination. Defense tactics can often succeed in making a key expert witness appear confused, less-than-authoritative, argumentative, surly, etc. Preparing experts who have had little or no prior experience on the witness stand for the rigors of cross-examination should be a paramount concern at pretrial conferences between the law enforcement members of the case team (especially the prosecutors) and the expert.

Useful tools for insuring effective expert witness management in preparation for cross examination include playing devil's advocate with the expert in technical discussions on the points he or she will cover on direct examination (this is a useful role for another expert, experienced at cross examination to assume with the prospective expert witness); asking the prospective expert witness to candidly discuss weaknesses in his or her own theories, positions or opinions; and engaging in one or more "full dress" rehearsals, i.e. mock cross-examination sessions, recorded, with other members of the team present as observers to later critique the expert's performance. Table 15 presents techniques for cross-examining an expert witness.

7.2.5 Anticipating Defense Objections and Impeachment Tactics

Sound management of prospective expert witnesses must include anticipating possible defense objections to the witness' credentials or authority aimed at preventing him or her from being accepted as an expert witness, or in the alternative, defense efforts to impeach the witness' credibility. The process of anticipating such tactics must be a central theme at one or more pretrial conferences held with the expert.

Table 15

Probable Techniques to Expect from Opposing Counsel when Cross-examining the Government's Expert Witness

A. Preparation for cross-examination of an expert imperatively requires:

1. the obtaining of the expert's report or the substance of the expert's testimony by pretrial investigation or discovery;

2. consultation with your own expert, who can help you

    a. understand what the other side's expert is saying;

    b. find holes in it; and

    c. identify recognized standard texts containing assertions of opinion inconsistent with those of the opponent's expert.

B. Armed with an inconsistent statement in a reputable textbook, counsel might ask the prosecution expert:

1. whether the expert recognizes the text as a standard and reputable work;

2. whether the expert has read it;

3. whether the expert read it in preparing his testimony for trial;

4. whether it supports the opinion which the expert has given;

5. whether the expert agrees with the statement just read;

6. whether the expert thinks that it supports the opinion to which the expert has testified;

7. whether it is not in fact inconsistent with the opinion to which the expert has just testified; and

8. for an explanation of the inconsistency.

Broadly speaking, objections to the expert's status as expert witness can take the shape of challenges to his or her formal credentials, prior relevant experience, familiarity with current technological developments in the field, etc. A thorough review of the expert's qualifications and a verification of the currency of his or her knowledge base are, as noted previously in this Manual, essential background steps for the team to complete and review.

Attempts to impeach the expert's credibility with the judge or jury will center on any of the following three allegations:

- lack of competence,
- bias, and
- financial interest in the outcome of the litigation.

Of course, the facts and circumstances of each case, and the situation with regard to each expert, will dictate whether one or more of these grounds for impeachment are invoked by the defense. However, with regard to impeachment for lack of competence, efforts to challenge the authoritativeness of the expert's views versus the views of rivals, and efforts to show that the expert is not familiar with the work of others prominent in the field, or with the latest developments in the field are common tactics. Their use should be anticipated and countered by adequate pre-litigation preparation.4/

Likewise, attempts to impeach for bias can be anticipated where the expert is a Government employee, has testified frequently for the prosecution in such cases and infrequently (or never) for the defense, or has previously published or stated prosecution-oriented views.5/ Moreover, if the Government's expert refuses to meet pretrial with defense representatives--which he is not obligated to do--allegations of bias can be expected to result.6/ Here, too, an adequate preparation at the pretrial stage can counter such impeachment tactics accepted by the court and/or credited by the jury. Table 16 presents some common objections to expert testimony.

Impeachment with regard to financial interest can be effective if the defense can show that the expert is paid a fee for his services, makes considerable income from such fees as a consultant to the prosecution (or from a steady salary as a Government employee), or that the fee is contingent upon a conviction in the case (which implies that the expert will espouse views most damaging to the defense and therefore partisan or biased).7/ Impeachment of expert witnesses for financial interest in business related litigation is a major danger and should be anticipated when agreeing to the level of compensation and basis for payment.

Table 16

Potential Trial Objections That Can Be Raised in A Computer Related Prosecution

- Hearsay
- Leading & suggestive
- Asked & answered*
- Cumulative
- No proper foundation
- Argumentative
- Irrelevant
- Immaterial
- Assuming facts not in evidence
- Beyond the scope
- Calling for a conclusion
- Incompetent
- Not the best evidence
- Privileged communication
- Self-incriminatory
- Opinion by non-expert
- Unintelligible
- Compound
- Self-serving
- Impeachment of own witness
- No corpus delecti
- Answer is non-responsive

* sometimes cumulative, sometimes not

blank page

FOOTNOTES

Section 1.0

1. S.240, "The Federal Computer Systems Protection Act of 1979", 96th Cong., 1st Sess. (1979).

2. United States Department of Justice, National Criminal Justice Information and Statistics Service, Computer Crime Criminal Justice Resource Manual (Washington, DC: US Government Printing Office, 1979) (hereinafter cited as "Computer Crime Manual") at 3.

3. August Bequai, Computer Crime (Lexington, MA: DC Heath & Co., 1978) (hereinafter cited as "Bequai") at 4.

4. Computer Crime Manual, supra note 2, at 4. (Donn B. Parker, noted computer crime researcher and author, served as Project Director and principal author of the Manual.)

5. Bequai, supra note 3, at _.

6. See Bequai, supra note 3, at 2-3.

7. Bequai, supra note 3, at 9-17.

8. Computer Crime Manual, supra note 2, at 4.

9. See Computer Crime Manual, supra note 2.

10. Donn B. Parker, "A Look at Computer Fraud and Embezzlement in Banking", The Magazine of Bank Administration (May 1976) at 21-22.

11. Statement of Richard Thornburgh, then Attorney General, as reported in Thomas Whiteside, Computer Capers, (New York, NY: Thomas Y. Crowell Co., 1978).

12. Ibid.

13. Chamber of Commerce of the United States, White Collar Crime (Washington, DC: Chamber of Commerce of the United States, 1974) at 6.

14. Bequai, supra note 3, at 181-194.

15. See Donn B. Parker, Susan H. Nycum, and S. Stephen Oura, Computer Abuse (Menlo Park, CA: SRI International, 1973) (distributed by the US Department of Commerce, Springfield, VA, 1973).

16. *Ibid*.

17. Bequai, *supra* note 3, at xiii.

18. Donn B. Parker, "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems", *Proceedings, 1976 National Computer Conference* (Arlington, VA: AFIPS Press, 1976). *See also* Computer Crime Manual, *supra* note 2, at 54.

19. Computer Crime Manual, *supra* note 2, at 31.

Section 2.0

1. *Random House Dictionary of the English Language*, college *edition (unabridged) (6th revised ed. 1968)* (hereinafter cited as "Random House Dictionary") at 465.

2. Henry Campbell Black, M.A., *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence*, Ancient and Modern (St. Paul, MN: West *Publishing Co.*, revised 4th Ed., 1968) (hereinafter cited as *"Black's Law Dictionary*) at 688.

3. Random House Dictionary, *supra* note 1, at 289.

4. *Id*. at 21.

5. *Id*. at 1261.

6. Black's Law Dictionary, *supra* note 2, at 688-89.

7. United States Department of Justice, National Criminal Justice Information and Statistics Service, *Computer Crime Criminal Justice Resource Manual* (Washington, DC: US *Government Printing Office, 1979*) at 307 (Appendix D).

Section 4.0

1. National District Attorneys' Association, *The Prosecutor's Manual on Economic Crime* (Chicago, IL: National District *Attorneys' Association*, 1977).

2. *Ibid*.

3. *Ibid*.

4. This is the current practice of the Office of Justice Assistance, Research and Statistics (OJARS) of the U.S. Department of Justice (DOJ), under which LEAA has been administratively located. For further information on how DOJ and LEAA calculate the reasonableness of expert consultants' requests for daily fee rates by tying these to professional income, it is suggested that contact be made with the Office of the Comptroller, DOJ, Washington, D.C.

5. For general discussion of the often complex question of when a pretrial expert becomes a potential expert witness--and his identity and views thereby become subject to pretrial discovery--in State litigation, *see* American Bar Association, *The Section of Litigation Outline Series*, "No. 2: *The Role of Experts in Business Litigation*" (Chicago, IL: ABA 1980) (hereinafter cited as "ABA Litigation Outline") at 11-30.

6. *See generally* ABA Litigation Outline, *supra* note 5, at Chapter V, "Discovery Proceedings Directed at Experts".

7. J.D. Kogan, J.D., "On Being A Good Expert Witness in A Criminal Case", *Journal of Forensic Science* (Jan., 1978) (hereinafter cited as "Kogan") at 195.

8. *See generally* ABA Litigation Outline, *supra* note 5, at Chapter V.

9. Kogan, *supra* note 7, at 195; *see also* ABA Litigation Outline, *supra* note 5, at 33-34.

10. *See generally* ABA Litigation Outline, *supra* note 5, at Chapter V.

11. Kogan, *supra* note 7, at 195; *see also* ABA Litigation Outline, *supra* note 5, at 33-34.

12. Kogan, *supra* note 7, at 194; ABA Litigation Outline, *supra* note 5, at 11-15, 29.

13. Kogan, *supra* note 7, at 195; *see also* California District Attorneys' Association, *Lay and Expert Witness Manual* (Sacramento, CA: CDAA, 1978).

14. Michael H. Graham, "Impeaching the Professional Expert Witness by a Showing of Financial Interest", 53 Ind. L.J. 35, 44-47 (Winter, 1977) (hereinafter cited as "Graham"); Kogan, *supra* note 7, at 198.

15. *See* Graham, *supra* note 14, at 45-47.

16. *See* ABA Litigation Outline, *supra* note 5, at Chapter V; *see also* Kogan, *supra* note 7, at 198.

17. Kogan, *supra* note 7, at 195. *See generally*, Lay and Expert Witness Manual, *supra* note 13.

18. Kogan, *supra* note 7, at 194. *See generally*, Lay and Expert Witness Manual, *supra* note 13.

19. ABA Litigation Outline, *supra* note 5, at 11-30; *see also* Kogan, *supra* note 7, at 198.

20. ABA Litigation Outline, *supra* note 5, at 11-30.

Section 5.0

1. *See*, for example, the so-called "Pinkerton Act," Public Law 89-554, 5 U.S.C. Sec.53.

2. 5 Code of Federal Regulations Sec.735 (1979).

3. 18 United States Code Sec.735 (1979).

4. Exchange National Bank of Chicago v. Abramson, 295 F. Supp. 87 (1969).

5. 17 Code of Federal Regulations Sec.240.10b-5 (1979).

6. *Cady, Roberts & Co*., 40 S.E.C. 907, 917 (1961).

7. Shapiro v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 495 F.2d 228 (2d Cir. 1974).

8. Chiarella v. United States, 48 U.S.L.W. 4250 (1980).

9. 18 United States Code Sec.798 (1976).

10. 50 United States Code (app.) Sec.781-85 (1975).

11. 18 United States Code Sec.1905 (1975).

12. *See*, 5 United States Code Sec.552(a) (1976). The Act's Criminal Penalties also apply to Government contractors. These, however, are defined in subsection (m) of the Act in such a way as to make them inapplicable to expert witnesses and consultants.

13. 13 United States Code Sec.214 (1976).

14. 26 United States Code Sec.7213, 7217 (1976).

15. 15 United States Code Sec.1681 *et seq*, (1976).

16. 20 United States Code Sec.1232 (q) (1976).

17. Public law 95-630, Title XI Sec.1101 (Nov. 10, 1978), *codified as* 92 Stat. 3697 (1978).

18. *Restatement of Torts (Second)* Sec.588 (1965).

19. Korb v. Kowaleviocz, 402 A.2d 897 (1979).

20. Adams v. Park, 403 A.2d 840 (1979).

21. Kennedy v. Cannon, 182 A.2d 54, 229 Md. 92 (1962).

22. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

23. *See* Stamicarbon, N.V. v. American Cynaimid Co., 506 F.2d 532, 540 M.11 (2d Cir. 1974).

24. Mycolex Corp. of America v. Pempo Corp. et al., 64 F. Supp. 420 (1946).

25. Kewanee Oil Co. v. Bicron Corp., 470 U.S. 416 (1974).

26. Restatement of Torts, Sec.757(b) (1938).

27. *See Federal Rules of Evidence*, R.501.

28. R.508, *Federal Rules of Evidence* (Supreme Court Draft).

29. *Federal Rules of Evidence* (March 1971 Draft).

30. R.509, *Federal Rules of Evidence* (Supreme Court Draft).

31. 345 U.S. 1 (1952).

32. R.703, *Federal Rules of Evidence*.

33. *See* American Bar Association, *Section of Litigation, Outline Series*, *"No. 2: The Role of Experts in Business Litigation"* (Chicago, IL: ABA, 1980) at 11-30.

34. R.26(b)(4), *Federal Rules of Civil Procedure*.

35. R.16(b), *Federal Rules of Criminal Procedure*.

36. Berkery Photo, Inc. v. Eastman Kodak Co., 1977 - 2 Trade Cases 72, 821, para. 61, 689 (S.D.N.Y. June 1, 1977).

37. Notable is OMB Circular A-71, Transmittal Memorandum No. 1: *Security of Federal Automated Information Systems* (July 27, 1978).

38. Executive Order No. 12, 1965.

39 FPM Letter 732-7: *Personnel Security Program for Positions Associated with Federal Computer Systems* (November 14, 1978).

Section 6.0

1. Kirby v. Illinois, 406 U.S. 602, 689 (1972).

2. *See* American Bar Association, *Section of Litigation Outline Series*, "No. 2: The Role of Experts in Business Litigation" (Chicago, IL: ABA, 1980) at 41-43.

3. *Id.* at 35-40.

4. *See* Gordon H. Miller, Esq., *Prosecutor's Manual on Computer Crimes* (Decatur, GA: Prosecuting Attorneys' Council of Georgia, 1978) at 20-23; August Bequai, Esq., *Computer Crime* (Lexington, MA: D.C. Heath and Co., 1978) at 117-143.

Section 7.0

1. Rule 7-109C, *American Bar Association Code of Professional Responsibility* (1969). *But see* Person v. Ass'n of the Bar of New York, 554 F. 2d 534 (2d. Cir. 1977) (Summary declaration of unconstitutionality of ABA Rule 7-109C).

2. M. Graham, "Impeaching the Professional Expert Witness by A Showing of Financial Interest," 53 *Ind. L.J.* 35, 43-45 (Winter 1977)(hereinafter cited as "Graham").

3. J.D. Koban, J.D., "On Being A Good Expert Witness in A Criminal Case", *Journal of Forensic Science* (Jan., 1978)(hereinafter cited as "Kogan") at 191-92.

4. American Bar Association, *Section of Litigation Outline Series*, "No. 2: The Role of Experts in Business Litigation" (Chicago, IL: ABA, 1980) at 31-32; *see also* Kogan, *supra* note 3, at 192-94.

5. Graham, *supra* note 2, at 43-45; Kogan, *supra* note 3, at 198.

6. Kogan, *supra* note 3, at 198.

7. Graham, *supra* note 2, at 42-45 and 50; Kogan, *supra* note 3, at 198.

* * *

BIBLIOGRAPHY

Akin, Richard H. The Private Investigator's Basic Manual. Springfield, Illinois: Charles C. Thomas, 1976.

Allen, Brandt. "Embezzler's Guide to the Computer." Harvard Business Review, July-August, 1975.

Allen, Brandt R. "Computer Fraud." Financial Executive 39 May 1971. p.38-43.

American Bar Association Section of Litigation. Litigation Outline Series, No. 2: "The Role of Experts in Business Litigation." Chicago, Illinois: American Bar Association, 1977.

Anderson, Ronald A., and Kumpf, Walter A. Business Law. Cincinnati, Ohio: South-Western Publishing Co., 1972.

Awad, Elias M., and Data Processing Management Association. Automatic Data Processing-Principles and Procedures. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1973.

Barmash, Isadore, ed. Great Business Disasters: Swindlers, Bunglers, and Frauds in American Industry. Chicago: Playboy Press, 1972.

Baruch, Hurd. Wall Street Security Risk. Washington, D.C.: Acropolis Books, 1971.

Becker, Jay. The Investigation of Computer Crime. Report prepared for Battelle Law and Justice Study Center, Seattle, Washington, 1978.

Becker, Robert S. The Data Processing Security Game. New York: Pergamon Press, 1977.

Benson, George C.S., and Engerman, Thomas S. Amoral America. Stanford, California: Hoover Institution Press, 1975.

Bequai, August. Computer Crime. Lexington, Massachusetts: D.C. Heath, 1977.

Bequai, August. White Collar Crime: A Twentieth Century Crisis. Lexington, Massachusetts: D.C. Heath, 1978.

Bequai, August. Organized Crime: The Fifth Estate. Lexington, Massachusetts: D.C. Heath, 1979.

Bequai, August. The Cashless Society: EFTS at the Crossroads. New York: John Wiley & Sons, 1980.

Bequai, August. "Litigation under the EFTS." *Federal Bar News* 23, June 1976. p.174-177.

Bequai, August. "Crooks and Computers." *Trial Magazine* 12, August 1976. p. 48-53.

Bequai, August. "Wanted: The White Collar Ring." *Student Lawyer* 5, May 1977. p.44-48.

Bequai, August. "The Binary Burglars." *Student Lawyer* 5, February 1977. p.18-24.

Bequai, August. "White Collar Plea Bargaining." *Trial Magazine* 13, July 1977. p.38-43.

Bequai, August. "Legal Problems in Prosecuting Computer Crimes." *Security Management* 21, July 1977. p.26-27.

Bequai, August. "White Collar Muggers Have Reason to Feel Safe." *Barrister* 4, Summer 1977. p.26-29.

Bequai, August. "The Forty Billion Dollar Caper." *Police Chief* XLIV, September 1977. p.66-68.

Bequai, August. "Computer Fraud: An Analysis for Law Enforcement." *Police Chief* XLIII, September 1976. p.54-57.

Bequai, August. "The Cashless Society: An Analysis of the Threat of Crime and the Invasion of Privacy." *University of Utah Journal of Contemporary Law* 3, Winter 1976. p.46-60.

Bequai, August. "The Electronic Criminal." *Barrister* 4, Winter 1977. p.8-12.

Bequai, August. "The Impact of EFTS on Our Criminal Justice System." *Federal Bar Journal* 35, Summer 1976. p.190-205.

Bequai, August. "Prosecutorial Decision-Making." *Police Law Quarterly* 4, October 1974. p.34-42.

Binns, James. "The Internal Auditor's Role in Questioning Fraud Suspects, Part I." *The Magazine of Bank Administration*, October, 1977.

Blake, Ian F., and Walker, Bruce J. *Computer Security and Protection Structures*. Stroudsburg, Pennsylvania: Dowden, Hutchinson & Ross, Inc., 1977.

Canadian Institute of Chartered Accountants. *Computer Audit Guidelines and Computer Control Guidelines*. Toronto, Canada: 1970.

Carroll, John M. Computer Security. Los Angeles: Security World Publishing Co., Inc., 1977.

Comptroller General of the United States, Report to the Congress. Computer Related Crimes in Federal Programs. U.S. General Accounting Office, 1976.

Coughran, Edward H. "Prosecuting Computer Abuse." Criminal Justice Journal, Vol. 1, 1978.

Davis, Keagle W., Mair, William C., and Wood, Donald R. Computer Control & Audit. The Institute of Internal Auditors, Inc., 1976.

Finch, James H., "Espionage and Theft Using Computers." Assets Protection, Vol. 2, No. 1., 1976.

Glick, Rush G., and Newsom, Robert S. Fraud Investigation. Springfield, Illinois: Charles C. Thomas, 1974.

Graham, Michael H. "Impeaching the Professional Expert Witness by a Showing of Financial Interest." Indiana Law Journal 53, 1975. p.35.

Hagen, Roger E. The Intelligence Process and White-Collar Crime. Report prepared for Battelle Law and Justice Study Center, Seattle, Washington, 1978.

Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1977.

Hoyt, Douglas. Computer Security Handbook. New York: Macmillan Information, 1973.

IBM. Data Security and Data Processing, Volume 5, Study Results. IBM, (No. G320-1375).

Inbau, Fred E., Moessens, Andre A., and Vitullo, Louis R. Scientific Police Investigation. Philadelphia: Chilton Book Co., 1972.

Jancura, Elise G. and Berger, Arnold H. Computers, Auditing & Control. Philadelphia: Auerbach, 1973.

Kirk, Paul L. and Thornton, John I., editors. Crime Investigation (second edition). New York: John Wiley & Sons, 1974.

Krauss, Leonard I. SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. New York: AMACOM, American Management Associations, 1973.

Leninger, Sheryl, editor. Internal Theft: Investigation and Control, An Anthology. Los Angeles: Security World Publishing Co., Inc., 1975.

Liebholz, Stephen and Wilson, Louis. Users Guide to Computer Crime. Philadelphia: Chilton Book Co., 1974.

Martin, James. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, New Jersey: Prentice-Hall, 1973.

Mettler, George B. Criminal Investigation. Boston: Holbrook Press, Inc., 1977.

Miller, Gordon H. Prosecutor's Manual on Computer Crimes. Decatur, Georgia: Prosecuting Attorneys' Council of Georgia, 1978.

O'Hara, Charles E. Fundamentals of Criminal Investigation (second edition). Springfield, Illinois: Charles C. Thomas, 1970.

O'Neill, Robert. Investigative Planning. Report prepared for Battelle Law and Justice Study Center, Seattle, Washington, 1978.

Osborn, Albert S. Questioned Document Problems. Albany, New York: Boyd Printing Company, 1944.

Parker, Donn B. Computer Abuse Assessment. A Stanford Research Institute report prepared for the National Science Foundation, Washington, D.C., 1975.

Parker, Donn B. Crime by Computer. New York: Charles Scribner's Sons, 1976.

Ralston, Anthony, ed. and Meek, Chester L., asst. ed. Encyclopedia of Computer Science. New York: Petrocelli/Charter, 1976.

Ruthberg, Zella G., ed. Audit and Evaluation of Computer Security. U.S. Dept. of Commerce, National Bureau of Standards, (NBS No. 500-19), 1977.

Shaw, Paul D., "Investigative Accounting." Assets Protection, Vol.3. No. 1, Spring 1978.

SRI International. Computer Crime-Criminal Justice Resource Manual. Produced under contract to the National Criminal Justice Information and Statistics Service. GPO, 1979.

The Institute of Internal Auditors. Systems Auditability and Control Study. A three part report prepared by Stanford Research Institute under a grant from IBM Corporation, The Institute of Internal Auditors, Inc., 1977.

The Investigation of White-Collar Crime: A Manual for Law-Enforcement Agencies. Produced by Battelle Law and Justice Study Center under Grant No. 76-Ta-99-0011. The manual may be ordered from: U.S. Government Printing Office, Washington, D.C. 20402, Stock No. 027-000-00507-1.

Vandiver, James V., "Forensic References." *Assets Protection*, Vol. 2. No. 4, Winter 1977.

VanTassel, Dennis. *Computer Security Management*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1972.

Walker, Bruce J. and Blake, Ian F. *Computer Security and Protection Structures*. Stroudsburg, Pennsylvania: Dowden, Hutchinson & Ross, Inc., 1977.

Whiteside, Thomas. *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. New York: Thomas Y. Crowell Company, 1978.

blank page

APPENDIX A

SIGNIFICANT ISSUES IN FEDERAL EXPERT WITNESS LAW

Appendix A addresses various issues of expert witness law in the Federal system. Among these are the significance of, and criteria for, designation as an expert witness, and limitations upon the subject matter and form of expert witness testimony. All issues of expert witness law are, of course, issues of law.

As a general rule, a witness at trial may testify only upon matters as to which he has personal first-hand knowledge, and only as to facts. The significance of the designation as an expert witness is that a witness who qualifies as an expert may testify in the form of opinions.

The applicable Federal Rule notes that such an individual may testify in the form of an opinion or otherwise.[1] The Advisory Committee's Note to that Rule makes the point that an expert witness is not confined to opinion testimony.[2] The role of an expert witness may, in whole or in part, be simply to provide general background--to give, for example, an exposition of scientific or other principles relevant to the case.

Under Federal Rules of Evidence, a witness may be justified as an expert by knowledge, skill, experience, training, or education.[3] This represents a relatively liberal standard, not confined necessarily to specific credentials. The Fifth Circuit in 1978, for example, in a prosecution for importing marihuana where the Government has to prove that the marihuana came from outside the customs territory of the United States, held that the trial judge had properly admitted the testimony of an expert whose qualifications came entirely from "the experience of being around a great deal and smoking it."[4] Titles are not dispositive one way or the other, as in the following two illustrations which, though admittedly predating the passage of the Federal

---

[1] Federal R. Evid. 702.

[2] Advisory Committee's Note to Federal R. Evid. 702.

[3] See Note 1, supra.

[4] United States v. Johnson, 575 F.2d 1347, 1360-61 (5th Cir. 1978).

Rules, are Federal appellate decisions.

In the first, the court held that the trial judge had erred in excluding testimony by a pipefitter, who had thirty-three years experience, on the ground that he was not a metal-weightist.[5] In the second, the court held a railroad fireman unqualified to express an opinion as to the distance within which the defendant's train could have been stopped, for although he held the position of a railroad fireman, his experience had been largely confined to operations in a railroad yard.[6]

Whether a witness will be deemed qualified to testify as an expert is decided by the trial judge.[7] The Supreme Court has recognized in the trial judge broad discretion in the admission or exclusion of expert evidence, and has posited that his action is to be sustained unless manifestly erroneous.[8]

Rule 702 of the Federal Rules of Evidence states, "(i)f scientific, technical, or other specialized knowledge will assist the trier-of-fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise." The Rule encompasses the two fundamental issues of expert witness law, "On this subject can a jury from this person receive appreciable help?"[9] The standard as to witness qualifications is a relatively liberal one; the expert's expertise must, of course, go to the area of his or her testimony. The standard as to the subject matter, i.e., whether expert testimony will assist the trier-of-fact, has similarly been characterized as somewhat broadening the range of admissibility.[10]

---

[5] Cunningham v. Gans, 507 F.2d 496 (2d Cir. 1974).

[6] Swift v. Southern Railway Co., 307 F.2d 315, 320 (4th Cir. 1962).

[7] Fed. R. Evid. 104(a).

[8] Salem v. United States Lines, 370 U.S. 31 (1962). See also, United States v. Lopez, 543 F.2d 1156, 1158 (5th Cir. 1976); Fernandez v. Chios Shipping Co., Ltd. 542 F.2d 145, 153 (2d Cir. 1976); Soo Line Railroad Co. v. Franhouf Corp., 547 F.2d 1365, 1374 (8th Cir. 1977).

[9] Wigmore, Evidence 1293 at 21 (3d ed. 1940). (Emphasis in original)

[10] United States v. Lopez, 543 F.2d at 1158.

An alternate and more restrictive standard recognized in some prior case law, and still of some influence, would require that the expert testimony, to be admissible, be on a subject which is beyond lay comprehension, that is, that the expert testimony be not only helpful but necessary to the trier-of-fact. The standard enunciated in the Federal Rules is one of helpfulness. As the Advisory Committee notes, "(w)hen opinions are excluded, it is because they are unhelpful and therefore superfluous and a waste of time."[11]

In a rėlated view, expert evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.[12] Furthermore, evidence, though admissible, is still subject to attack as to the weight it should be accorded by the trier-of-fact.[13]

Federal Rule of Evidence 702 can be found verbatim in the 1974 Uniform Rules of Evidence, and in the evidence rules of 13 States.[14]

Four other aspects of expert witness law are worthy of note. First, the Federal Rules of evidence do away with the ultimate issues rule, a rule characterized as having been honored as much in the breach as in the observance.[15] Rule 704 states, "(t)estimony in the form of an opinion or inference otherwise admissible is not objectionable because it embraces an ultimate issue to be decided by the trier-of-fact." Rule 704 has been adopted verbatim into the 1974 Uniform Rules of Evidence and in the evidence rules of 14 States.[16] The requirement remains that the opinion assist the trier-of-fact to understand the evidence or to determine a fact in issue.

---

[11] See Note 2, supra.

[12] Fed. R. Evid. 403, recognized as applicable to expert testimony in United States v. Fosher, 590 F.2d 381, 383 (1st Cir. 1979); United States v. Green, 548 F.2d 1261, 1268 (6th Cir. 1977); United States v. Sisvo, 543 F.2d 837, 844 (8th Cir. 1979).

[13] Singer Co. v. E.L. DuPont de Nemours and Co., 579 F.2d 433, (8th Cir. 1979).

[14] These States are Arizona, Arkansas, Maine, Minnesota, Montana, Nebraska, New Mexico, North Dakota, Oklahoma, South Dakota, Washington, Wisconsin, and Wyoming.

[15] Project of a Committee on New York Trial Lawyers, Recommendation and Study Relating to the Advisory Committee's Preliminary Draft of the Proposed Federal Rules of Evidence 205 (June 1, 1970).

Second, Rule 703 of the Federal Rules of Evidence states, in pertinent part, that "(t)he facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to him at or before the hearing." Expert opinion could previously be elicited only by way of hypothetical questions posed to the expert in examination at trial, or by reference in examination at trial to personal knowledge possessed by the expert, such as a doctor's personal knowledge of his patient. Federal Rule 703 expands the possibility of allowing opinions based on facts to be made known to the expert witness not only at, but before trial as well. The Rule thus legitimizes opinions based on hypotheticals before trial, on trial or deposition transcripts, and/or on observations from attendance at trial.[17]

Third, Rule 703 also states that "(i)f of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject, the fact or data need not be admissible in evidence." Inadmissible evidence and evidence not in the record including hearsay and matters that violate the best evidence rule, may thus be the basis for expert testimony.[18] An expert witness will typically be asked whether he or she routinely relies on such data, and whether others in his or her field do likewise, whether he as well as others would act upon the information for purposes other than testifying in a lawsuit. The reliance exercised by the particular field of experts must, moreover, be reasonable. Thus, opinions based on data reasonably relied upon by physicians would ordinarily be recognized, while the opinion of an "accidentologist" as to the point of impact in an automobile collision, based on statements by bystanders, would not.[19] While an expert witness may and ordinarily will rely in some fashion on the opinions of others, he may not merely summarize or act as a conduit for introduction of such hearsay opinions; the data may be relied upon, but only in forming his or her own opinion. Rule 703 has been adopted without change in the

---

[16] These States are Arizona, Arkansas, Maine, Michigan, Minnesota, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, Washington, Wisconsin, and Wyoming.

[17] But see Fed. R. Evid. 615, Exclusion of Witnesses.

[18] United States v. Brown, 548 F.2d 1194 (5th Cir. 1977); United States v. Sims, 514 F.2d 147 (9th Cir. 1975).

[19] Advisory Committee's Note to Fed. R. Evid. 703.

Uniform Rules of Evidence and in the evidence rules of 14 States.[20]

Fourth, and finally, Rule 705 of the Federal Rules of Evidence states, "(t)he expert may testify in terms of opinion or inference and give his reasons therefore without prior disclosure of the underlying facts or data, unless the court requires otherwise. The expert may, in any event, be required to disclose the underlying facts or data on cross-examination."[21] The Rule states that the facts or data underlying an expert opinion need not be brought out on direct examination, unless the judge so requires. The Advisory Committee characterizes the Rule as a corollary to the recognition of other forms of expert testimony than the hypothetical question (Rule 703).[22] The Advisory Committee recognizes that the Rule might place an opposing party in a difficult position, if not for the opportunities for pretrial discovery.[23] The scope of pretrial discovery, the importance of which is thus increased by the Rule, is examined at length in Appendix B. Rule 705 has been adopted without change in the Uniform Rules of Evidence and in the evidence rules of nine States.[24]

---

[20] These States are Arizona, Arkansas, Maine, Minnesota, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, South Dakota, Washington, Wisconsin, and Wyoming.

[21] Also pertinent to the matter of expert witnesses is Fed. R. Evid. 706, Court Appointed Experts.

[22] Advisory's Committee's Note to Fed. R. Evid. 705.

[23] Ibid.

[24] These States are Arkansas, Arizona, Michigan, Minnesota, Montana, North Dakota, Oklahoma, Washington, and Wyoming.

blank page

APPENDIX B

FEDERAL PRETRIAL AND TRIAL DISCOVERY ISSUES APPLICABLE TO COMPUTER RELATED CRIME CASES

1.0 INTRODUCTION

This Appendix identifies and examines pretrial and trial discovery issues relating to the use of expert witnesses and consultants in Federal cases. It addresses the question, when and according to what procedures, the defendant in a criminal or civil case will be permitted access to information, directly or indirectly from, or regarding, the prosecution's or plaintiff's expert witnesses or consultants. The approach is in two parts, treating first the law applicable to criminal cases, and second, the law applicable to civil cases.

2.0 THE CRIMINAL SETTING

Discovery under the Federal Rules of Criminal Procedure is narrowly circumscribed. The rules provide for discovery by a defendant of four types of information: (1) statements of the defendant, (2) the defendant's prior record, (3) documents and tangible objects, and (4) reports of examinations and tests. Only the latter two are directly pertinent to expert information.[1]

2.1 Discovery of Documents and Tangible Objects

The most significant provision as regards expert information is one which limits the discovery of documents and tangible objects. This provision stipulates that the rule authorizing the discovery of such information "does not authorize the discovery of inspection of reports, memoranda or other internal government documents made by the attorney for the Government or other Government agents in connection with the investigation or prosecution of the case, or of statements made by Government witnesses or prospective witnesses except as provided in 18 U.S.C. 3500."[2] The exception provided in 18 U.S.C. 3500 represents the Jencks Act, which will be examined later.

Two amendments considered but not adopted by Congress will place into sharper focus the scope and effect of this limitation. In 1975 the Supreme Court proposed, and the Congress considered, amendments to the Federal Rules of Criminal Procedure. One amendment proposed by the Court,[3] and adopted in modified form by the House of Representatives, would have required the following--that on the request of a defendant, the Government furnish a written list of the names and addresses of all intended Government witnesses, together with records of any known prior felony convictions on their parts.[4] The Congress ultimately chose not to adopt any such amendment. The Joint Explanatory Statement of the Committee on Conference noted that a majority of the Conferees believed it not in the interest of the effective administration of criminal justice to require that the Government or defendant be forced to reveal the names and addresses of its witnesses before trial.[5]

In the opinion of one appellate court the fact that such an amendment was initially proposed and deleted by Congress did not preclude district court discretion to compel pretrial disclosure of the identity of Government witnesses. The court held, however, that such authority is appealable for abuse of discretion, and reversed the lower court on the facts of that case.[6]

The Congress considered also an amendment which would have narrowed the limitation precluding discovery of "reports, memoranda, or other internal Government documents made by the attorney for the Government or other Government agents" to one precluding merely "the mental impressions, conclusions, opinions, or legal theories of the attorney for the Government or other Government agents."[7] This amended wording, which paralleled the more liberal discovery provision applicable in civil cases, was likewise not adopted by the Congress.

2.2 Discovery of Expert Information

There are three possible, specific avenues to discovery of expert information. First, by statute a defendent has the right in capital cases to be provided by the Government three days in advance of trial, or earlier if justice requires, the names and addresses of witnesses.[8] It has been held that a case is not capital if the Government expressly disclaims any intention of seeking the death penalty.[9] It has been held also that, where the failure to provide a witness name before trial was not negligent and not prejudicial, there was no reversible error.[10]

Second, the limitation upon the discovery of documents and tangible objects does not apply to the discovery of reports of examinations and tests.[11] To be discoverable such reports must have been made in connection with the particular case, and must be material to the preparation of the defense or intended for use by the Government as evidence in chief at trial.[12] In one case noncompliance with a specific request for a voice comparison test was held not to be reversible error, where it had been the opinion of the expert that the quality of the recordings was too poor to render a decision one way or the other. The court held that the evidence was thus not material and its denial not prejudicial.[13] The 1966 Committee Notes made clear that, as the defendant may be unaware of what examinations or tests have been made, he was not required to designate particular items sought.[14] The same may be assumed to be true under the 1975 amendments. The provision for discovery of reports of examinations and tests constitutes a potentially significant, though limited, avenue to discovery of expert information.

Where a party intends to introduce computer-obtained evidence, the Manual for Complex and Multidistrict Litigation states, "(i)t is essential that the underlying data used in the analyses, programs and programming method and all relevant computer inputs and outputs be made available to the opposing party far in advance of trial. This procedure is required in the interest of fairness and should facilitate the introduction of admissible computer evidence. Such procedure provides the adverse party and the court with an opportunity to test and examine the inputs, the program and all outputs prior to trial.[15]

The Second Circuit in 1970 considered a case wherein the defendant had requested at trial and been denied the computer program on the basis of which a prosecution expert witness had testified.[16] The court noted the apparent correctness of the computer evidence, and similar considerations, on the basis of which it declined to reverse the conviction.[17] The court in dictum, however, placed "the Government on the clearest possible notice of its obligation (if it should tender a witness to state the results of a computer's operation, to have the program available for defense scrutiny and use on cross-examination) and also of the great desirability of making the program and other materials needed for cross-examination of computer witnesses, such as flow-charts used in the preparation of programs, available to the defense a reasonable time before trial.[18]

The First Circuit in 1978 cited this opinion, and stated in dictum that the Government is well-advised that notice of an intention to use computer data should be given well in advance.[19] No notice had been given, but the court there similarly declined to reverse the conviction in light of the apparent simplicity of the computer program and the minimal prejudice to the defendant.[20]

The Sixth Circuit in a 1973 opinion emphasized in dictum the need for pretrial discovery where computer evidence is to be introduced. Its basis for declining to reverse the conviction on such grounds was that the defendant had made neither a motion for discovery as to scientific tests nor a motion for a continuance to permit expert witnesses of his choosing to conduct their own tests.[21]

Finally, the Third Circuit in 1975, in a failure to file income tax returns prosecution, held that IRS non-filers lists were not discoverable to impeach the reliability of IRS computers.[22] The court recognized in dictum that pretrial discovery of information material for the defense of a criminal prosecution may take precedence over the privacy interests of persons having no connection with a case and to whom the information sought pertains.[23] The court held the information non-discoverable in this case, however, in light of the tendency the information might have to obscure at trial the real issue in the case, and in light of the alternative information available to the defense.[24] The Government, both voluntarily and as a result of the district court's order, had offered the defendant alternative information, including computer handbooks, statistical analyses, experts familiar with non-filers lists and IRS computer procedures, and an opportunity to perform test runs on the IRS computers.[25]

A third avenue to discovery of expert information is constitutional due process. There are circumstances under which the Government is obligated, under the constitution and for reasons of due process, to disclose information to the defense.[26] The Supreme Court has enunciated that the determining factor is whether the information would have an effect on the outcome of the trial.[27] In a subsequent case the Court set forth the following conditions: (1) that there had been suppression of evidence by the prosecution after a defense request for production, (2) that the evidence is favorable to the defendant, and (3) that the evidence is material to the issues of guilt and punishment.[28] In a case more recent still, the court elaborated more broadly and fully the applicable standards.[29] None of these cases, however, have involved expert information.

In one opinion the Supreme Court reversed a murder conviction, where the defense had been denied pretrial discovery of the defendant's clothing, containing stains characterized by the prosecution's blood-identification expert, in trial testimony, as human blood of the victim's type.[30] The stains were in reality, paint, a fact known to the prosecution at the time of trial. While constitutional due process does represent an avenue to discovery, and is of evolving import, it is by its nature of limited applicability both generally and as regards expert information.

2.3 Limitations On Discovery

Two other aspects of the Federal Rules of Criminal Procedure are to be noted. The rules provide that upon a sufficient showing, the court may at any time order that the discovery or inspection be denied, restricted, or deferred, or make such other order as is appropriate.[31] The court may also permit a party, upon motion, to make the necessary showing in whole or in part in the form of a written statement to be inspected by the judge alone.[32]

Secondly, the Rules make provision for failure by a party to comply with the discovery mandates of the rules.[33] In such an instance the court may order the noncomplying party to permit the discovery or inspection, grant a continuance, or prohibit the party from introducing evidence not disclosed, or it may enter such other order as it deems just under the circumstances.[34] One court has stated that a mistrial should not be declared on the basis of non-compliance with discovery orders, and that declaration of a mistrial should base further retrial under the double jeopardy clause of the Constitution.[35]

2.4 The Jencks Act

A next-to-last subject for consideration is the Jencks Act.[36] While, as noted above, reference is made to the Act in the Federal Rules of Criminal Procedure, the Act is a significant statutory provision in its own right.[37] The Act precludes pretrial discovery in criminal cases of statements or reports made by Government witnesses or prospective witnesses, and in the possession of the Government.[38] It at the same time requires that any such statements be available to the defense, once the witness has testified on direct examination at trial.[39] If the Government elects not to do so, the court is directed to strike the testimony of the witness from the record or, if justice requires, to declare a mistrial.[40]

While the Act requires that statements of a witness be available to the defense once the witness has testified on direct examination at trial, there are two limitations, both of which have received some considerable elaboration in the courts. The first is that the statement must relate to the subject matter as to which witness has testified.[41] The second concerns the scope of the term "statement" as used in the Act. The Act defines "statement" for its purposes as (1) written and adopted by the witness, or (2) a substantially verbatum and contemporaneous recording of an oral statement by the witness, or (3) a recording or transcription of a statement made by the witness to a grand jury.[42] The courts have tended to be liberal in their interpretation of the second. A valuable analysis is to be found in the Supreme Court opinion in Paterno v. United States, handed down less than two years subsequent to passage of the Act.[43]

As to the Act's prohibition upon pretrial discovery, several courts have considered the potential conflict between this prohibition which provides for discovery by a defendant of statements made by him or her. A number of courts have held that the Jencks Act prohibits pretrial disclosure of witness statements even when such statements contain quotations allegedly attributable to defendant, thus resolving such a conflict in favor of the Jencks Act.[44] The relation between the Jencks Act and Federal Rule 16 (a)(1)(D), which provides for pretrial discovery of reports of examinations and tests, and whether there necessarily exists any tension between the two, is, on the other hand, not entirely clear.

While the Jencks Act concerns Government witnesses, the Supreme Court in 1974 considered an issue involving a defense witness in an opinion worthy of note.[45] In that case a defense investigator had been called as a witness by the defense to impeach the testimony of prosecution witnesses, from whom he had previously obtained statements. The Court held that the District Court had acted within its authority in ordering that relevant portions of the investigator's report be made available to the prosecution, and that otherwise, the investigator would not be permitted to testify about his interviews with the witnesses. The Court held that Rule 16 of the Federal Rules of Criminal Procedure was inapplicable as a protection against trial discovery, for the reason that its provisions govern pretrial procedures, and do not extend into the trial context.[46] The Court held that the qualified privilege derived from the attorney work-product doctrine similarly afforded no protection to the report, in that calling the investigator as a witness constituted a waiver of work-product immunity with respect to matters covered in his testimony.[47]

Another form and basis for discovery at trial of expert information is provided by Federal Rule of Evidence 612, which applies to both criminal and civil cases, and is considered in the examination of the civil setting below.

3.0 THE CIVIL SETTING

The rules applicable to discovery in civil litigation are decidely and understandably more liberal than those applicable in criminal litigation. The Federal Rules of Civil Procedure state that, in general, parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter in the pending action.[48] For purposes of pretrial discovery, the scope of relevancy includes information which, though not admissible as evidence, may lead to admissible evidence.

3.1 Forms Of Pretrial Discovery Applicable To Expert Witnesses

While the Federal Rules of Civil Procedure delineate six forms of pretrial discovery,[49] only two--depositions upon oral examinations,[50] and depositions upon written examinations[50]--are applicable to nonparties, such as expert witnesses. As to experts, the Federal Rules of Civil Procedure provide a specific rule.[52] Before turning to that rule, however, three other provisions of the Rules are worth noting.

3.1.1 Production of Documents by Parties

First, in Rule 34, which is applicable only to parties, and which pertains to production of documents and things. This rule has been interpreted to include computer tapes.[53] In an action involving allegedly racially discriminatory employment practices, the plaintiff moved for an order compelling production of the defendant's current computerized master payroll file and all computer print-outs for W-2 forms of the defendant's employees. The defendant objected on the basis that the information sought constituted a trade secret. The court held that because of accuracy and inexpensiveness of producing the requested documents, it would require the defendant to produce them, but would entertain a motion, if the defendant desired, to put the documents under protective order.[54] The Advisory Committee Note to Rule 34 states in pertinent part, "The inclusive description of 'documents' is revised to accord with changing technology." It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form.

In many instances, this means that respondent will have to supply a print-out of computer data. The burden thus placed on respondent will vary from case to case, and the courts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs.

Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of non-discoverable matters, and costs.[55] Rule 34 is circumscribed, as are all the discovery provisions under the Federal Rules of Civil Procedure, by the general limitations as to relevancy and privilege. In pretrial civil discovery in computer related litigation, Rule 34 is not uncommonly invoked together with Rule 26(b)(4), which pertains to experts.

Second, is Rule 26(b)(3) which stipulated limitations upon, and standards specific to, discovery of "documents and tangible things...prepared in anticipation of litigation or for trial by or for another party or by or for that party's representative (including his attorney, consultant, surety, indemnitor, insurer, or agent)."[56] Known as the work-product doctrine, this provision is applicable to discovery under Rule 34 above. The Advisory Committee's Notes, however, expressly declare the work-product doctrine inapplicable to the discovery of facts known and opinions held by experts.[57]

Third is Rule 26(c) which provides that a party or person from whom discovery is sought may move for a protective order to avoid "annoyance, embarrassment, oppression, or undue burden or expense." The rule enumerates protective orders of eight types, including "that the discovery not be had...that certain matters not be inquired into, or that scope of the discovery be limited to certain matters...that a trade secret or other confidential research, development, or commercial information not be disclosed or be disclosed only in a designated way."[58] The Rules make provision additionally for objections to specific questions during the course of an oral or written deposition.[59]

3.1.2 Discovery from Expert Witnesses not Parties

As to experts, the Federal Rules of Civil Procedure provide a specific rule.[60] It is this Rule, and not standards relevant either to work-product or attorney-client privilege which shall govern the discovery of facts known and opinions held by experts.[61] It has been held that the identity of an expert who falls within the scope of the Rule is freely discoverable subject only to the general limitations upon discovery, since the matter of identity falls outside the introductory language of the Rule.[62]

The Rule does not apply to the expert whose information was not acquired in preparation for trial but rather because he was an actor or viewer with respect to transactions or occurrences that are part of the subject matter of the lawsuit. Such an expert should be treated as an ordinary witness.[63] Nor does the Rule apply to experts who are themselves parties.[64] Such experts should be treated according to the rules applicable to parties. Nor does the Rule apply to experts who were informally consulted in preparation for trial, but not retained or specially employed.[65] As to such experts the Rules provide virtually no basis for discovery.[66] The Rule will apply to an in-house expert if but only if some part of the expert's work is to concern itself with the litigation.[67]

The Rule specifically applicable to facts known and opinions held by experts, is subject to the general limitations upon discovery as to relevance and privilege, and is limited to facts and opinions acquired or developed in anticipation of litigation.[68] The Rule distinguishes two categories of experts and establishes distinct rules for each. The first category consists of each person whom a party expects to call as an expert witness at trial.[68] The second consists of each expert who has been retained or especially employed by another party in anticipation of litigation or preparation at trial.[70] If an expert has been retained to work upon, and has worked upon, several aspects of a case, but is expected to testify upon only certain of these, it has been held that the first category's standards will apply as to those aspects upon which he is expected to testify, and the second category's standards otherwise.[71]

Discovery of facts known and opinions held by experts of the second type will be permitted only upon a showing of exceptional circumstances under which it is impractical for the party seeking discovery to obtain facts or opinions on the same subject by other means.[72]

Discovery of facts known and opinions held by experts of the first type is governed by a two-step process. A party may through interrogatories require any other party to state the subject matter and the substance of the facts and opinions, as to which each such expert is expected to testify, together with a summary of the grounds for each opinion.[73] Since this written summary of an expert's opinion and its basis will be prepared by the attorney presenting the expert, it is likely to be cursory. Thereafter, upon motion, and subject to its discretion, a court may decide to order further discovery by other means.[74]

Certain courts have chosen to exercise that discretion in favor of liberal discovery. One such court invoked the liberal spirit pervading the Federal Rules of Civil Procedure and held that once the traditional problem of allowing one party to obtain the benefit of another's expert cheaply has been solved, there is no reason to treat an expert differently than any other witness.[75] The opinion in another case noted the highly technical nature of the lawsuit and stated that the expert testimony would be crucial to the resolution of the complex and technical factual disputes in the case, and that effective cross-examination would be essential.[76]

Other courts have chosen to exercise that discretion conservatively. One court refusing to order further discovery put forward a standard of "compelling need."[77] Two other courts refusing to order further discovery set forth as the standard to be met a showing of substantial need and undue hardship in obtaining the information elsewhere.[78] In one of these cases, to encourage the court to deny the motion, counsel for the party resisting discovery provided both the reports and the questions to which they were prepared for the court to inspect in camera without prejudice to any claim of privilege that might be asserted later.[79]

So are decided the discoverability of experts' reports and or experts, pursuant to Rule 26(b)(4)(A)(ii), which, it might be noted, was incorporated into the Federal Rules of Civil Procedure in 1970.

Certain federal district courts have adopted local rules for the disclosure in civil cases of reports of expert witnesses as an element of pretrial preparation.[80] A judge may also in pretrial conference require on-going exchanges of information. In one case a judge disallowed an expert's testimony, in consequence of the party's failing to give pretrial notice, as ordered, of all experts and their reports.[81] Two civil cases involving pretrial discovery issues relating to computer experts are Perma Research and Development Co. v. Singer Co.,[82] and Pearl Brewing Co. v. Jos. Schiltz Brewing Co.[83]

3.2 Discovery At Trial

A final subject is Rule 612 of the Federal Rules of Evidence. This Rule, applicable to both criminal and civil litigation, concerns trial discovery. The Rule requires that if a witness while testifying uses a writing to refresh his memory the writing must be made available to the other party. The significance of the rule is that it additionally permits the court in its discretion to make available to the opposing party writings used by a witness to trial, to refresh his memory for the purpose of testifying. In a recent case the court considered a motion to compel production of notebooks, prepared by the attorney in anticipation of trial, and furnished to an expert witness prior to trial not as a basis for testimony or to refresh the witness' memory, but merely as general background.[84] The judge ultimately declined to order the materials to be made available to the other party, in part because the attorney may not have realized the potential import of the rule. The judge emphasized, however, that "there will be hereafter powerful reason to hold that materials considered work products should be withheld from prospective witnesses if they are to be withheld from opposing parties."[85] Whether the Rule will be similarly applied elsewhere and in the future is to be observed. The Berkery case does, at least, highlight the discretion afforded by the Rule and the potential consequences of that discretion.

4.0 FOOTNOTES TO APPENDIX B

1. Fed. R. Cr. P. 16(a)(1).

2. Fed. R. Cr. P. 16(a)(2).

3. Proposed Rule 16(a)(1)(E).

4. H.R. 6799.

5. Joint Explanatory Statement of the Committee of Conference, Cong. Res. H-7682-7683 (July 28, 1975).

Many states have statutes which require that the accused be notified prior to trial of the witness to be used against him. These include Alaska, Arizona, Arkansas, California, Colorado, Florida, Idaho, Wisconsin, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, Oklahoma, Oregon, Tennessee and Utah. See Advisory Committee Note to Proposed 1975 Amendments to Fed. R. Cr. P.

6. United States v. Connone, 528 F.2d 296 (1975).

7. See note 4, supra.

8. 18 U.S.C. § 3432.

9. Hall v. United States, 410 F.2d 253, 660 (4th Cir. 1969).

10. Gregory v. United States, 369 F.2d 185, 187-188 (D.C. ir. 1966).

11. See note 2, supra.

12. Fed. R. Cr. P. 16(a)(1)(D).

13. United States v. Fontaine, 575 F.2d 970 (1st Cir. 1978).

14. 1966 Committee Note to Subd. (a)(2).

15. Manual for Complex and Multidistrict Litigation (Admin. Off. U.S. Courts 1969).

16. United States v. Dioguardi, 428 F.2d 1033 (2d Cir. 1970).

17. Ibid. at 1038, 1039.

18. Ibid. at 1038.

19. United States v. Cepeds Penes, 577 F.2d 754, 761 (1st Cir. 1978).

20. Ibid.

21. United States v. Russo, 480 F.2d 1228, 1241-43 (6th Cir. 1973).

22. United States v. Liebert, 519 F.2d 542 (3d Cir. 1975).

23. Ibid. at 549-550.

24. Ibid. at 550-551.

25. Ibid.

26. Brady v. Maryland, 373 U.S. 83 (1963).

27. Giles v. Maryland, 386 U.S. 66 (1967).

28. Moore v. Illinois, 408 U.S. 786 (1972).

29. United States v. Agurs, 427 U.S. 97 (1976).

30. Miller v. Pate, 386 U.S. 1 (1967).

31. Fed. R. Cr. P. 16(d)(7).

32. Ibid.

33. Fed. R. Cr. P. 16(d)(2).

34. Ibid.

35. Harris v. Young, 607 F.2d 1081 (4th Cir. 1979).

36. 18 U.S.C. § 3500.

37. See note 2, supra.

38. 18 U.S.C. § 3500 (a).

39. 18 U.S.C. § 3500 (b) (c).

40. 18 U.S.C. § 3500 (d).

41. See Note 39, supra.

42. 18 U.S.C. § 3500 (e).

43. 360 U.S. 343 (1959).

44. United States v. Walk, 533 F.2d 417 (9th Cir. 1975); United States v. Feinberg, 502 F.2d 1180 (7th Cir. 1974); United States v. Wilkerson, 456 F.2d 57 (8th Cir. 1972).

45. United States v. Nobles, 422 U.S. 225 (1975).

46. Ibid. at 234-236.

47. Ibid. at 236-240.

48. Fed. R. Civ. P. 26(b)(1).

49. Fed. R. Civ. P. 30,31,33,34,35,36.

50. Fed. R. Civ. P. 30.

51. Fed. R. Civ. P. 31.

52. Fed. R. Civ. P. 26(b)(4).

53. Adams v. Dan River Mills, Inc. 54 F.R.D. 220 (W.D. Vade 1972).

54. Ibid.

55. Advisory Committee's Note to 1970 Amendments to Rule 34.

56. Fed. R. Civ. P. 26(b)(3).

57. Advisory Committee's Note to 1974 Amendments, Rule 26 (b) (4).

58. Fed. R. Civ. P. 26(c).

59. Fed. R. Civ. P. 30(c), 31(b).

60. See Note 52, supra.

61. See Note 57, supra.

62. Baki v. B.F. Diamond Construction Co., 71 F.R.D. 179 (D. Md. 1976); Sea Colony, Inc. v. Continental Insurance Co., 63 F.R.D. 113 (D. Del. 1974) Conta Perry v. W.S. Darley & Co., 54 F.R.D. 278 (E.D. Wis. 1971).

63. Advisory Committee's Note to 1974 Amendments, Rule 26(b) (4); Duke Gardens Foundation, Inc. v. Universal Restoration, Inc., 52 F.R.D. 365 (S.D. N.Y. 1971); Perry v. W.S. Darley & Co., 54 F.R.D. 278 (E.D. Wisc. 1971).

64. Rodriques v. Hrinds, 56 F.R.D. 11 (W.D. Pa. 1972).

65. Advisory Committee's Note to 1974 amendment's, Rule 26 (b)(4); Nemetz v. Aye, 63 F.R.D. 66 (W.D. Pa. 1974).

66. Ibid.

67. Seiffer v. Topsy's International, Inc. 69 F.R.D. 69 (D. Ken 1975); Virginia Electric & Power Co. v. Sun Shipbuilding & D.D. Co., 68 F.R.D. 397 (E.D. Va. 1975).

68. See Note 52, *supra*.

69. Fed. R. Civ. P. 26(b)(4)(A).

70. Fed. R. Civ. P. 26(b)(4)(B).

71. Bailey v. Meister Bran Inc., 57 F.R.D. 11 (N.D.W. 1972); Inspirations Consolidated Copper Co. v. Lumbermens Mutual Casualty Co., 60 F.R.D. 205 (S.D.N. 1973).

72. See Note 70, *supra*.

73. Fed. R. Civ. P. 26(b)(4)(A)(i).

74. Fed. R. Civ. P. 26(b)(4)(A)(ii).

75. Herbst v. International Telephone & Telegraph Corp., 65 F.R.D. 528 (D. Conn. 1975).

76. Quadrini v. Sikorsky Aircraft Division, United Aircraft Corp., 74 R.D. 594 (D. Conn. 1977).

77. United States v. 145.31 Acres of Land, 54 F.R.D. 359 (M.D. Pa. 1972).

78. Wilson v. Resnick, 51 F.R.D. 510 (E.D. Pa. 1970), Breedlove v. Beech Aircraft Corp., 57 F.R.D. 202 (N.D. Miss. 1972).

79. Breedlove v. Beech Aircraft Corp., 57 F.R.D. 202.

80. See Graham *Discovery on Experts Under Rule 26(b)(4) on the Federal Rules of Civil Procedure Part One, An Analytical Study*, 1976 U.ILL.L.F. 895, 93 & n. 136; n. 137 summarizes State law regarding discovery of experts.

81. Tabatchnick v. G.D. Searle & Company, 67 F.R.D. 49 (D.N.V. 1975).

82. 542 F.2d 111 (2d Cir. 1976). See Note on Singer, 43 Brook L.R. 1119 (1976).

83. 415 F. Supp. 1122 (S.D. Tex. 1976).

84. Berkery Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263 (2d Cir. 1979).

85. Ibid.

APPENDIX C

FEDERAL AND STATE CASES
REGARDING USE OF EXPERT WITNESSES

Testimony by experts has been admitted into evidence on a broad range of subjects:

1. The mental capacity or condition of a person, *U.S. v. Davis*, 523 F.2d 1265 (5th Cir. 1975): the results of compulsory psychiatric examinations are admissible on the issue of sanity, but the use of an incriminating statement made during a compulsory examination is impermissible on the issue of guilt; *Gibson v. Zahradnick*, 581 F.2d 75 (4th Cir.),cert. denied, 439 U.S. 996 (1978) (and cases cited therein); but see *U.S. v. Reason*, 549 F.2d 309 (4th Cir. 1977); *U.S. v. Reifsteck*, 535 F.2d 1030 (8th Cir. 1976); *U.S. v. Matos*, 409 F.2d 1245 (2d Cir. 1969), cert. denied, 397 U.S. 927 (1970); that experts may differ in their opinions concerning the mental condition of a defendant does not mean, in and of itself, that there is a reasonable doubt as to sanity, *U.S. v. Urbanis*, 490 F.2d 384, 386 (9th Cir.), cert. denied, 416 U.S. 944 (1974); *U.S. v. Ortiz*, 488 F.2d 175 (9th Cir. 1973). The issue of a defendant's mental condition should be determined from all the evidence rather than from the opinions of experts alone, *U.S. v. Fortune*, 513 F.2d 883, 890-891 (5th Cir.), cert. denied, 423 U.S. 1020 (1975); *Mims v. U.S.*, 375 F.2d 135, 143 (5th Cir. 1967).

2. The teachings and purposes of the Communist Party, *Frankfeld v. U.S.*, 198 F.2d 679 (4th Cir. 1952), cert. denied, 344 U.S. 922 (1953).

3. Current propaganda themes, *U.S. v. German-American Vocational League, Inc.*, 153 F.2d 860 (3d Cir.), cert. denied, 328 U.S. 833 (1946).

4. Value of particular property, *Sartor v. Arkansas Natural Gas Corp.*, 321 U.S. 620, 627 (1944).

5. Cause of death, *Clay County Cotton Co. v. Home Life Insurance Co.*, 113 F.2d 856 (8th Cir. 1940).

6. Bookkeeping and income tax returns, *U.S. v. Gray*, 507 F.2d 1013 (5th Cir.), cert. denied, 423 U.S. 824 (1975); *U.S. v. Augustine*, 189 F.2d 587 (3d Cir. 1951).

7. Retail value of consumer goods, *Cave v. U.S.*, 390 F.2d 58 (8th Cir.), cert. denied, 392 U.S. 906 (1968).

8. Markings and stamps on bank checks, *U.S. v. Mustin*, 369 F.2d 626 (7th Cir. 1966).

9. Mechanics of how the numbers game or bookmaking organizations operate, U.S. v. Barletta, 565 F.2d 985 (8th Cir. 1977) (testimony of an FBI agent who had done considerable investigative work in the area); Moore v. U.S., 394 F.2d 818 (5th Cir. 1968), cert. denied, 393 U.S. 1030 (1969); see U.S. v. Scavo, 593 F. 2d 837 (8th Cir. 1979) (agent allowed to testify as to defendant's role in bookmaking operation).

10. The modus operandi of criminal schemes, U.S. v. Stull, 521 F.2d 687 (6th Cir. 1975), cert. denied, 423 U.S. 1059 (1976) (testimony of postal inspector describing a mail fraud scheme); U.S. v. Jackson, 425 F.2d 574 (D.C. Cir. 1970) (testimony of operation of pickpocket scheme).

11. Handwriting, U.S. v. Reece, 547 F.2d 432 (8th Cir. 1977); U.S. v. Green, 523 F.2d 229 (2d Cir. 1975), cert. denied, 423 U.S. 1074 (1976); U.S. v. Galvin, 394 F.2d 228 (3d Cir. 1968); U.S. v. Acosta 369 F.2d 41 (4th Cir. 1966), cert. denied, 386 U.S. 921 (1967); Wood v. U.S., 357 F.2d 425 (10th Cir.), cert. denied, 385 U.S. 866 (1966).

12. The technical operation of the United States Mint, U.S. v. Sheiner, 410 F.2d 337 (2d Cir.), cert. denied, 396 U.S. 825 (1969).

13. The ineffectiveness of a weight-reducing drug, U.S. v. Andreadis 366 F.2d 423 (2d Cir. 1966), cert. denied, 385 U.S. 1001 (1967).

14. Spectrograms or "Voiceprints," U.S. v. Williams, 583 F.2d 1194 (2d Cir. 1978), cert. denied, 439 U.S. 1117 (1979); U.S. v. Baller, 519 F.2d 463 (4th Cir.), cert. denied, 423 U.S. 1019 (1975); U.S. v. Franks, 511 F.2d 25 (6th Cir.), cert. denied, 422 U.S. 1042 (1975); but see U.S. v. Addison, 498 F.2d 741 (D.C. Cir. 1974) (spectrographic identification not then sufficiently accepted in scientific community).

15. The operation of equipment for the purpose of producing counterfeit currency, U.S. v. Wilson, 451 F.2d 209 (5th Cir. 1971), cert. denied, 405 U.S. 1032 (1972).

16. The genuineness of Government bonds, U.S. v. Martin, 459 F.2d 1009 (9th Cir.), cert. denied, 409 U.S. 864 (1972).

17. The source of marihuana, U.S. v. Johnson, 575 F.2d 1347 (5th Cir 1978), cert. denied, 440 U.S. 907 (1979).

18. Firearms and ballistics, Davis v. Freels, 583 F.2d 337 (7th Cir. 1978); U.S. v. Bowers, 534 F.2d 186 (9th Cir.), cert. denied, 429 U.S. 942 (1976).

19. Architecture, *Scholz Homes, Inc. v. Wallace*, 590 F.2d 860 (10th Cir. 1979).

20. Valuation of pecuniary loss, *Driscoll v. U.S.* 456 F. Supp. 143 (D. Del. 1978), aff'd 605 F. 2d 1195 (1979); *D'Angelo v. U.S.*, 456 F. Supp. 127 (D. Del. 1978), aff'd 605 F.2d 1194 (1979).

21. Aircraft, *Dychalo v. Copperloy Corp.*, 78 F.R.D. 146 (E.D. Pa.), aff'd, 588 F.2d 820 (1978) (safety of loading ramp).

22. Defective products, *Nanda v. Ford Motor Co.*, 509 F.2d 213 (7th Cir. 1974).

23. Design, *Soo Line R. R. Co. v. Fruehauf, Corp.*, 547 F. 2d 1365, 1375-1376 (8th Cir. 1977) (design of railroad cars); *Holmgren v. Massey-Ferguson, Inc.*, 516 F.2d 856 (8th Cir. 1975) (defective design of corn picker).

24. Law, *U.S. v. Sturgis*, 578 F.2d 1296 (9th Cir.), cert. denied, 439 U.S. 970 (1978) (sentences customarily imposed by State courts).

25. Narcotics, *U.S. v. Wolk*, 398 F. Supp. 405, 414-415 (E.D. Pa. 1975).

26. Photographs, *U.S. v. Sellers*, 566 F.2d 884 (4th Cir. 1977) expert on photographs allowed to assist the jury by explaining light, shadowy reflections).

An expert witness may identify and explain charts summarizing his own testimony or the testimony of other witnesses. *U.S. v. Gray*, 507 F.2d 1013 (5th Cir.), cert. denied, 423 U.S. 824 (1975); *U.S. v. Rath*, 406 F.2d 757 (6th Cir.), cert. denied, 394 U.S. 920 (1969). See also *U.S. v. Scales*, 594 F.2d 558 (6th Cir.), cert. denied, 441 U.S. 946 (1979) (expert not needed; agent who catalogued exhibit and who had knowledge of analysis of materials was permitted to summarize).

blank page

APPENDIX D

SELECTED STATE PRIVACY LAWS

APPLICABLE TO COMPUTER SECURITY

The following States have an array of privacy laws that will impact on computer security:

ALASKA - Constitution contains a "right to privacy" provision. Criminal Information Systems Regulations: Any person has the right to inspect, challenge, and correct information in a State criminal justice system of records that refers to him. Polygraph: Lie-detector test are prohibited in the private sector.

ARIZONA - Consumer Credit Reporting: Limits credit report distribution to "legitimate business transactions" unless authorized by court order or consent of the individual. Consumers are allowed access to their own credit reports to contest inaccuracies.

ARKANSAS - Criminal Information Systems Regulations: A criminal justice and highway safety information center oversees the Statewide information network containing criminal and motor vehicle records. Data subjects are guaranteed right of inspection and corroboration. Information Systems Regulation: A seven-member information practices board chaired by the Lieutenant Governor was established by Act 730 of 1975 to regulate State information practices. Under the act, information in State systems of records must be accurate, current, and relevant. Individuals have the right of inspection and contestation.

CALIFORNIA - An employee may now inspect most records in his personnel file--letters of reference and records of investigation for possible criminal offense are the only specific exceptions. Polygraph: Lie-detector tests are prohibited in the private sector.

CONNECTICUT - Arrest Record Expungement: All records of arrests that did not lead to prosecution or conviction must be erased. Polygraph: Lie-detector tests are prohibited in the private sector. Medical Records: Consent of the individual is required for access to mental health records.

DELAWARE - Arrest Record Expungement: A person may petition for expungement of all records relating to an arrest that did not lead to a conviction. Polygraph: Lie-detector tests are prohibited as a condition of employment in both public and private sectors.

FLORIDA - Arrest Record Expungement: Records of arrest that did not lead to conviction may be erased except for the one copy that is retained by the Department of Law Enforcement to aid in future investigations.

GEORGIA - Medical Records: Confidential medical records may be released only when required by law or with consent of the individual.

HAWAII - Arrest Record Expungement: Records of arrests that did not lead to conviction may be erased. Polygraph: Lie-detector tests are prohibited for both public and private employment.

IDAHO - Polygraph: Lie-detector tests are prohibited as a condition of employment in the private sector.

ILLINOIS - Arrest Record Expungement: Prospective private employers may not ask whether an applicant has an arrest record. Medical Records: Most public and private hospitals must provide copies of hospital records to former patients, their doctors, or attorneys. Polygraph: Lie-detector tests may not be required during the course of criminal trial.

IOWA - Criminal Information Systems Regulation: Criminal history records may only be distributed to criminal justice agencies. A person may examine information maintained about him, file for correction and deletion, and seek judicial review. Intelligence and surveillance data may not be stored on computer.

KANSAS - Consumer Credit Reporting: Credit reports may not be distributed for other than legitimate business reasons without a court order or an individual's consent. An individual may request a credit agency to disclose the nature, substance, source, and all recipients of the information. The right to contest or correct is enforced by the Consumer Credit Commissioner.

KENTUCKY - Consumer Credit Reporting: Credit agencies may not collect records of arrest that did not result in conviction.

LOUISIANA - Arrest Record Expungement: Records of an arrest for a misdemeanor that did not result in conviction may be sealed.

MAINE - Arrest Record Expungement: A person receiving full pardon of conviction may seek expungement of all records of the conviction.

MARYLAND - Arrest Record Expungement: An individual may seek expungement of any record of arrest, detention or confinement that was not followed by an official charge. Polygraph: Lie-detector tests are prohibited in the private sector as a condition of employment.

MASSACHUSETTS - Information Systems Regulation: The Information Practices Act of 1975 prevents inter-agency transfer of personal information unless authorized by the individual or required by State law; grants a person the right of access and contestation; and requires that any data maintained be accurate, complete, timely, pertinent, and relevant. Criminal Information Systems Regulation: A Criminal History Systems Board oversees and regulates criminal information systems within the State. Arrest Record Expungement: Records of criminal offense conviction on file in the office of the commissioner of probation may be destroyed. Records of arrest and conviction for a first violation of the Controlled Substances Act may be sealed. Polygraph: Lie-detector tests are prohibited for both public and private employment.

MICHIGAN - Polygraph: An employee may not be dismissed solely for refusing to take a lie-detector test.

MINNESOTA - Information Systems Regulation: Collection of information by State agencies is limited to that specifically required for authorized program administration and management. At the time of data collection a person must be informed of the purpose of the data collection, whether the data is legally required, and the consequences of supplying or refusing to supply the data.

MONTANA - Polygraph: Lie-detector tests may not be required as a condition of public employment.

NEBRASKA - Polygraph: A person employed by law enforcement agencies may be required to submit to lie-detector tests.

NEVADA - Arrest Record Expungement: A person convicted of a crime may petition to seal all records of conviction 15 years after conviction for a felony, 10 years after for a gross misdemeanor, and five years after for a misdemeanor. When arrest charges are dismissed or a defendant acquitted, all records may be sealed.

NEW JERSEY - Arrest Record Expungement: Records of arrests that did not lead to conviction for a high misdemeanor may be sealed. Polygraph: Lie-detector tests cannot be required as a condition of private employment.

NEW MEXICO - Arrest Record Expungement: Only law enforcement officials, the record subject, or his agent are allowed access to arrest records.

NORTH CAROLINA - Information Systems Regulation; Security safeguards must be installed before confidential data may be entered into a State agency computer. Arrest Record Expungement: A person placed on probation after pleading guilty to the Controlled

Substances Act may petition for sealing of all records relating to the arrest and conviction. A copy of the records will be kept by the Department of Justice for judges' eyes only.

OKLAHOMA - Consumer Credit Reporting: An individual has the right to inspect his credit file and must receive a copy of the report each time it is issued by the credit agency.

OREGON - Arrest Record Expungement: Records of conviction for Class C felony down to misdemeanor may be sealed. Polygraph: Lie-detector tests may not be required for public or private employment. Consumer Credit Reporting: Access to credit reports is limited to Government agencies, credit bureaus, creditors, and persons with written authorization from the consumer.

PENNSYLVANIA - Polygraph: Only law enforcement officials and persons having access to narcotics and dangerous drugs may be required to submit to lie-detector tests.

RHODE ISLAND - Polygraph: Lie-detector tests may not be required for public or private employement.

SOUTH CAROLINA - Arrest Record Expungement: All records of arrest are to be destroyed upon dismissal of charges or acquittal.

TENNESSEE - Medical Records: Hospital records are closed except when opened by court order, when good cause is shown by the patient, or when required for health department inspection.

UTAH - Information Systems Regulation: All State and local agencies that maintain information systems must file annual reports. Individuals have the right of inspection and correction. At the time of data collection, an individual must be informed of the purpose for collection, whether the data is legally required, and what penalties exist for refusing to supply the data.

WASHINGTON - Polygraph: Only law enforcement officers and persons handling controlled substances may be required to submit to lie-detector tests as a condition of employment.

WISCONSIN - Medical Records: In a personal injury proceeding, a court may order all pertinent medical records opened for inspection.

*U S GOVERNMENT PRINTING OFFICE: 1981 341-233/1691

blank page

U.S. Department of Justice
Bureau of Justice Statistics

Official Business
Penalty for Private Use $300

Postage and Fees Paid
U.S. Department of Justice
Jus 436
THIRD CLASS
BULK RATE

Washington, D.C. 20531